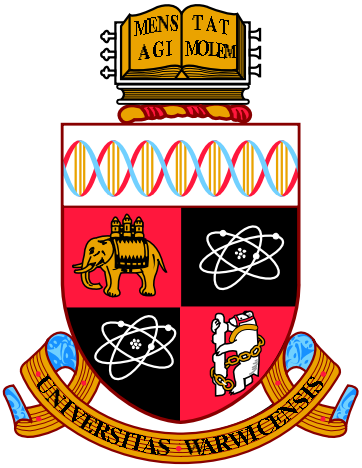

Minimal generation of transitive permutation groups

by

Gareth M. Tracey

Thesis

Submitted to the University of Warwick

for the degree of

Doctor of Philosophy

Mathematics Institute

4th May 2017

Contents

Acknowledgments

Nothing will ever be enough to fully thank my supervisor, Professor Derek Holt: without his patience in reading my proofs, his suggestions for new problems, and his encouragement to never give up on old ones, this thesis, and my enjoyment in writing it, would never have happened. If I turn out to be even a small fraction of the mathematician and person he is, then I will have had a very worthwhile career.

I would like to thank Dr. Dmitriy Rumynin for allowing me to give two algebra seminars, and also for writing countless letters of reference for me.

Along with Derek and Dmitriy, I have been extremely lucky to work with Professor Andrea Lucchini on a very enjoyable and productive research visit in Padova. I would like to thank the Università degli studi di Padova for their hospitality. I would also like to thank Andrea for his constant encouragement, and for writing many letters of reference for me.

Thank you to Professor Laci Pyber for giving me my first postdoctoral position, and for pointing me in the direction of some very interesting mathematics. I would also like to thank Dr. Tim Burness, not only for inviting me to give talks in Bristol and Bielefeld which were invaluable for telling people about my results, but also for his great work in Group Theory, much of which has inspired me as a young mathematician.

I would like to thank the Mathematics Institute at the University of Warwick, and in particular Carole Fisher, who have supported me, and provided a very enjoyable working environment for the past three and a half years. I would also like to thank the Department of Mathematics and Statistics at Maynooth University,

and in particular Dr. David Wraith, Dr. John Murray and Dr. Anthony Small, for introducing me to the wonderful world of Pure Mathematics. Thank you to the Engineering and Physical Sciences Research Council for their financial support.

On a personal level, my friends have made these past three and half years so enjoyable away from the blackboard. Matthew, Pedro, Chris, Florian, Celine, Daniel, Alex, James, Kathryn and Maike: I want to thank them sincerely for their friendship and support. I would also like to thank Four Masters Coventry Gaelic Football Club for warmly welcoming me into their team.

Special thanks though, are reserved for Steph. Words cannot express how happy she has made this last year of my Ph.D. I am so lucky to have met such an incredible person.

Finally, I would like to thank my parents Matt and Noeleen for always encouraging me to do what I love.

Declarations

I hereby certify that the material contained in this thesis is my own original work, except where otherwise stated, and that it has not been submitted in any previous application for a higher degree. Chapter 7 appears as an article in the *Journal of Algebra* [49].

I was admitted as a research student in September 2013 and as a candidate for the degree of Ph.D. in July 2014. The higher study for which this is a record was carried out in the Mathematics Institute at the University of Warwick between 2013 and 2017.

Abstract

This thesis discusses upper bounds on the minimal number of elements $d(G)$ required to generate a finite group G. We derive explicit upper bounds for the function d on transitive and minimally transitive permutation groups, in terms of their degree n. In the transitive case, bounds obtained first by Kovács and Newman, then by Bryant, Kovács and Robinson, and finally by Lucchini, Menegazzo and Morigi, show that $d(G) = O(n/\sqrt{\log n})$, for a transitive permutation group G of degree n. In this thesis, we find best possible estimates for the constant involved.

We also settle an old conjecture of Pyber on minimal generator numbers in minimally transitive permutation groups of degree n. Specifically, we prove that such a group can be generated by $\mu(n) + 1$ elements, where for an integer n with prime factorisation $n = \prod_{p \text{ prime}} p^{n(p)}$, $\mu(n) := \max_{p \text{ prime}}\{n(p)\}$. Furthermore, this bound is best possible.

We also derive upper bounds on the minimal number of elements $d_G(M)$ required to generate a submodule M of an induced module $V \uparrow_H^G$ for a finite group G and a subgroup $H \leq G$. These upper bounds are given in terms of the dimension $\dim V$, and the index $|G : H|$.

Finally, we prove that there exists a universal constant C such that if G is a transitive permutation group of degree $n \geq 2$, then $d(G) \leq Cn^2/(\log |G|\sqrt{\log n})$. This reduces another conjecture of Pyber on the number of subgroups of the symmetric group $\mathrm{Sym}(n)$. Moreover, we show that this bound is asymptotically best possible.

Chapter 1

Introduction

1.1 Background

A well-developed branch of finite group theory studies properties of certain classes of permutation groups as a function of their degree. The purpose of this thesis is to study one such property: the minimal size of a generating set.

For a finitely generated group G, let $d(G)$ denote the minimal number of elements required to generate G. Of course, one can study minimal generation for any type of algebraic object; in particular, the minimal size of generating set for a vector space V over a field $\mathbb{F}$, i.e. the $\mathbb{F}$-dimension of V. However, while the function $\dim_{\mathbb{F}}$ is well-behaved with respect to substructures (that is to say, W is a subspace of V implies that $\dim_{\mathbb{F}} W \leq \dim_{\mathbb{F}} V$), the same is not true for the function d on finite groups (the familiar example of $H := \langle (1,2), (3,4), \ldots, (2n-1, 2n) \rangle \leq \mathrm{Sym}\,(2n)$, with $n \geq 2$, suffices to demonstrate this: $d(H) = n$ while $d(\mathrm{Sym}\,(2n)) = 2$).

Similarly, while $\dim_{\mathbb{F}} V$ also equals the size of any irredundant set of generators for V, the same fails to hold for $d(G)$. (For a group G, a subset X of G is said to be an "irredundant generating set" for G if $\langle X \rangle = G$, and $\langle Y \rangle \neq G$ for each proper subset Y of X.) To see this, note that $\{(1,2), (2,3), \ldots, (n-1, n)\}$ is an irredundant set of generators in the symmetric group $\mathrm{Sym}\,(n)$. These phenomena mean that the function d is much more difficult to study, and as a result, requires deeper and more powerful techniques.

Apart from its independent interest, the invariant $d(G)$ is also useful in subgroup enumeration. Indeed, if G is a finite group and $d(H) \leq m$ for all subgroups H of G, then G has at most $|G|^m$ subgroups. This is often a crude upper bound, but the method can sometimes be used effectively if combined with other results.

In Chapter 7, we prove one of our main theorems, Theorem 1.2.3, whose motivation comes from a conjecture of L. Pyber which counts the number of subgroups of the symmetric group $\mathrm{Sym}(n)$, in terms of n (see Chapter 7 for more details).

1.2 Main results and layout of the thesis

Apart from Chapter 2, where we discuss some preliminary material in Representation Theory and in the theory of finite permutation groups, this thesis can be split up into two main parts, which we now discuss.

1.2.1 Part I: Generating minimally transitive groups

The purpose of this thesis is to study upper bounds on the minimal size of a generating set in certain classes of finite transitive permutation groups. We begin our analysis in Chapter 3, where we study the class of minimally transitive permutation groups (a *minimally transitive* permutation group is a transitive permutation group which contains no proper transitive subgroups). In [45], Pyber asks if every minimally transitive permutation group of degree n can be generated by $\mu(n)+1$ elements. Here, for an integer n with prime factorisation $n = \prod_{p \text{ prime}} p^{n(p)}$, we define

$$\mu(n) := \max_{p \text{ prime}} \{n(p)\}.$$

In Chapter 3, we answer this question in the affirmative.

Theorem 1.2.1. *Let G be a minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n)+1$.*

The main tool in proving the theorem is the method of "generator critical groups" developed by F. Dalla Volta and A. Lucchini (see [14], or Section 2 of the survey [41]). We remark that the theorem was proved by Pyber himself in the regular and nilpotent cases (see [45]), and by Lucchini in the soluble case (see [34]). Moreover, the bound in the theorem is best possible. To see this, let p be an odd prime, and set $G := V \rtimes \langle \tau \rangle$ to be the semi-direct product of an elementary abelian group V of order p^n with a cyclic group $\langle \tau \rangle$ of order 2, where τ acts by inverting the non-trivial elements in V. Then G is minimally transitive of degree $|G|$ (via the regular action) and $d(G) = n+1 = \mu(|G|)+1$. Finally, we remark that our proof relies on the Classification of Finite Simple Groups (which from here on in will be abbreviated to CFSG), via Lemma 3.4.1.

1.2.2 Part II: Generating transitive groups

The remainder of the thesis is devoted to the study of the behaviour of $d(G)$ on the more general class of transitive permutation groups. We prove two main results, in Chapters 6 and 7, which we now discuss.

The two main results

In [28], [8], [33] and [37], it is shown that $d(G) = O(n/\sqrt{\log n})$ whenever G is a transitive permutation group of degree $n \geq 2$ (here, and throughout this thesis, "log" means log to the base 2). A beautifully constructed family of examples due to L. Kovács and M. Newman shows that this bound is "asymptotically best possible" (see Example 6.3.2), thereby ending the hope that a bound of $d(G) = O(\log n)$ could be proved. (For an example of where this "hope" is discussed, see [4, Remark 6.4].)

The constants involved in these theorems, however, were never estimated. Our first main result in Part II reads as follows.

Theorem 1.2.2. *Let G be a transitive permutation group of degree $n \geq 2$. Then*

$$d(G) \leq c_1 n/\sqrt{\log n}$$

where $c_1 := \frac{\sqrt{3}}{2}$ in all but finitely many cases.

The theorem is stated more precisely as Theorem 6.1.3. In particular, we give details of the finitely many cases for which we were not able to prove the bound $d(G) \leq c_1 n/\sqrt{\log n}$. It is important to remark that although these finitely many cases could not be dealt with using our methods, we do not believe that they are genuine exceptions. For more details, see Chapter 6. Note also that the bound in Theorem 1.2.2 is attained when $n = 8$ and $G \cong D_8 \circ D_8$.

We prove Theorem 1.2.2 in Chapter 6. The proof relies on the CFSG indirectly through our application of Theorem 2.1.14.

Our second main result in Part II also involves upper bounds on $d(G)$ for transitive permutation groups G of degree n, but this time the bound obtained is an asymptotic one, and is expressed in terms of n and $|G|$. Specifically, we prove

Theorem 1.2.3. *There exists an absolute constant C such that*

$$d(G) \leq \left\lfloor \frac{Cn^2}{\log |G| \sqrt{\log n}} \right\rfloor$$

whenever G is a transitive permutation group of degree $n \geq 2$.

We prove Theorem 1.2.3 in Chapter 7, where we also show (see Example 7.3.3) that the bound is asymptotically best possible. As discussed briefly in Section 1.1, the motivation for Theorem 1.2.3 is a reduction of a conjecture of Pyber on the number of subgroups of $\mathrm{Sym}(n)$. See Chapter 7 for more details. We also remark that the proof of Theorem 1.2.3 relies on the CFSG, again through our application of Theorem 2.1.14.

Proving the main theorems in Part II

So how do we prove Theorems 1.2.2 and 1.2.3? We have the same hypothesis in each theorem, so for the purposes of this discussion fix a transitive permutation group G of degree $n \geq 2$. As we shall see in Chapters 6 and 7, both theorems follow from existing results in the literature when G is primitive. Thus the bulk of Part II concerns imprimitive G. So assume that G is imprimitive, with minimal block size $r \geq 2$. Then (see Chapter 2) G may be viewed as a certain subgroup of a wreath product $R \wr S$, where R is primitive of degree r, S is transitive of degree $s := n/r$, and $G\pi = S$, where $\pi : G \to S$ denotes projection over the top group. Write the base group of this wreath product as $B := R_{(1)} \times R_{(2)} \times \ldots \times R_{(s)}$, where each $R_{(i)} \cong R$, and for a subgroup L of R, write $B_L := L_{(1)} \times \ldots \times L_{(s)} \cong L^s$.

Rather than just studying imprimitive permutation groups, we will actually study the function $d(G)$ on the subgroups G of wreath products described above in a bit more generality. So while continuing to adopt the set-up introduced in the above paragraph, assume now that R is just an arbitrary non-trivial finite group (rather than a primitive permutation group). The idea is as follows: let L be a minimal normal subgroup of R. Then $G/G \cap B_L$ is isomorphic to a subgroup of $(R/L) \wr S$. Thus, we now have a path to an inductive argument: we just need to investigate the contribution of $G \cap B_L$ to $d(G)$ (of course, $d(G) \leq d(G \cap B_L) + d(G/G \cap B_L)$).

Since L is a minimal normal subgroup of a finite group, $L \cong T^a$ for some finite simple group T. If T is nonabelian, then $G \cap B_L$ is a minimal normal subgroup of G (see Lemma 6.2.5), and $d(G) \leq 1 + d(G/G \cap B_L)$ by a result of Lucchini (see Theorem 6.2.2). So assume that T is isomorphic to a cyclic group of order p, for p prime. Then B_L is an $\mathbb{F}_p[G]$-module, where $\mathbb{F}_p$ denotes the field of p elements. Let $H := N_G(R_{(1)}) = \pi^{-1}(\mathrm{Stab}_S(1))$. Then $|G : H| = s$ since $G\pi = S$ is transitive, and $L_{(1)}$ is an $\mathbb{F}_p[H]$-module. Moreover, $L_{(1)}$ generates B_L as a G-module, and $\dim B_L = as = |G : H| \dim L_{(1)}$. Hence (see Proposition 2.2.6) B_L is isomorphic to the induced module $L_{(1)} \uparrow_H^G$.

Let $d_G(G \cap B)$ denote the minimal number of elements required to generate $G \cap B$ as a G-module. Since $d(G) \leq d_G(G \cap B_L) + d(G/G \cap B_L)$, we now need to study another invariant: the minimal number of elements $d_G(M)$ required to generate a submodule M of an induced module $V \uparrow_H^G$, where $H \leq G$ are finite groups, and V is a finite dimensional H-module over an arbitrary field $\mathbb{F}$. In Chapter 5, which is the critical step of the thesis, we derive upper bounds on $d_G(M)$ in terms of $\dim V$ and $|G : H|$ (and some additional data when $char(\mathbb{F})$ is positive and/or the image of the induced action (say S) of G on the set $H\backslash G$ of right cosets of H in G is insoluble).

This demonstrates the importance of Chapter 5 of the thesis, but what about Chapter 4? In Chapter 4, we give a necessary condition for a transitive permutation group G of degree $2^m 3$ to be minimally transitive. But why do we care? Consider again the situation described above, that is, suppose that M is a submodule of an induced module $V \uparrow_H^G$, where $H \leq G$ are finite groups, and V is a finite dimensional H-module over an arbitrary field $\mathbb{F}$. Let S denote the image of the induced action of G on $H\backslash G$. Due to their nature, the main bounds obtained in Chapter 5 fail to prove Theorem 1.2.2 in the case when the degree $s = |G : H|$ of S is of the form $s = 2^m 3$, and S contains no soluble transitive subgroups. Thus, we need to work harder in this exceptional case. So assume that $s = 2^m 3$, and S contains no soluble transitive subgroups. If $\widetilde{G}$ is a subgroup of G acting transitively on $H\backslash G$, then $H\widetilde{G} = G$ so $V \uparrow_H^G \downarrow_{\widetilde{G}}$ is isomorphic to $V \uparrow_{\widetilde{G} \cap H}^{\widetilde{G}}$, by Mackey's Theorem (see Theorem 2.2.4). Thus, since $d_G(M) \leq d_{\widetilde{G}}(M)$, it is no loss, for the purposes of bounding $d_G(M)$, to assume that S is minimally transitive.

Therefore, some information on the structure of the minimally transitive permutation groups of degree $s = 2^m 3$ will be necessary. Our main result reads as follows.

Theorem 1.2.4. *Let G be a minimally transitive permutation group of degree $n = 2^m 3$. Then one of the following holds:*

(i) G is soluble, or:

(ii) G has a unique nonabelian chief factor, which is a direct product of copies of $L_2(p)$, where p is a Mersenne prime.

1.3 Notation and terminology

Our proofs are theoretical, although we do use MAGMA [6] for computations of generator numbers and composition factors for some groups of small order. In particular, we compute the maximum values of $d(G)$ as G runs over the transitive groups of degree n, for $2 \leq n \leq 32$. These values are presented in Table B.1 (Appendix B).

Notation: The following is a table of constants which will be used throughout the thesis.

b	$\sqrt{2/\pi} = 0.797885\ldots$
c_1	$\sqrt{3}/2 = 0.866025\ldots$
c	$1512660\sqrt{\log(2^{19}15)}/(2^{19}15) = 0.920581\ldots$
c_0	$\log_9 48 + (1/3)\log_9 24 = 2.24399\ldots$
c'	$\ln 2/1.25506 = 0.552282\ldots$

We will adopt the notation of [29] for group names, although we will usually write $\mathrm{Sym}(n)$ and $\mathrm{Alt}(n)$ for the symmetric and alternating groups of degree n. Furthermore, these groups, and their subgroups act naturally on the set $\{1, \ldots, n\}$; we will make no further mention of this.

The centre of a group G will be written as $Z(G)$, the Frattini subgroup as $\Phi(G)$, and the Fitting subgroup as $F(G)$. The letters G, H, and K will usually be used for groups, while U, V and W will usually be modules. The letter M will usually denote a submodule. Finally, group homomorphisms will be written on the right.

We finish by recording two definitions which will be used throughout the thesis.

Definition 1.3.1. Let G be a group.

(a) Write $a(G)$ to denote the composition length of G.

(b) Let $a_{ab}(G)$ denote the number of abelian composition factors of G.

(c) Let $c_{nonab}(G)$ denote the number of nonabelian chief factors of G.

Definition 1.3.2. For a positive integer s with prime factorisation $s = p_1^{r_1} p_2^{r_2} \ldots p_t^{r_t}$, set $\omega(s) := \sum r_i$, $\omega_1(s) := \sum r_i p_i$, $K(s) := \omega_1(s) - \omega(s) = \sum r_i(p_i - 1)$ and

$$\widetilde{\omega}(s) = \frac{s}{2^{K(s)}} \binom{K(s)}{\lfloor \frac{K(s)}{2} \rfloor}.$$

Chapter 2

Background

In this chapter, we outline some preliminary material which will be used throughout the thesis.

2.1 Permutation groups

2.1.1 Group actions and transitivity

We begin with an introduction to permutation group theory. For a set Ω, let $\mathrm{Sym}(\Omega)$ denote the group of permutations of Ω. We will write permutations on the right, and compose from left to right, so that when $g, h \in \mathrm{Sym}(\Omega)$, and $\omega \in \Omega$, we have $\omega^{gh} = (\omega^g)^h$.

Definition 2.1.1. A subgroup G of $\mathrm{Sym}(\Omega)$ is called a *permutation group on* Ω.

An *action* of a group G on Ω is a homomorphism $\theta : G \to \mathrm{Sym}(\Omega)$. In the special case when $\Omega = H\backslash G$ is the set of right cosets of a subgroup H of G, we will write the associated action as $\theta_H : G \to \mathrm{Sym}(\Omega)$. In this case, we call Ω the *coset space* of H in G.

Definition 2.1.2. We say that two actions $\theta_1 : G_1 \to \mathrm{Sym}(\Omega_1)$ and $\theta_2 : G_2 \to \mathrm{Sym}(\Omega_2)$ are *permutation isomorphic*, and write $(G_1, \theta_1) \cong (G_2, \theta_2)$, if there exists a group isomorphism $\alpha : G_1 \to G_2$, and a bijection $\sigma : \Omega_1 \to \Omega_2$ satisfying $\sigma(\omega^{g\theta_1}) = \sigma(\omega)^{g\alpha\theta_2}$ for all $\omega \in \Omega_1$, $g \in G_1$.

We remark that when the homomorphisms θ_1 and θ_2 are understood, we will write $(G_1, \Omega_1) \cong (G_2, \Omega_2)$. Note also that two permutation groups on a set Ω are permutation isomorphic if and only if they are conjugate as subgroups of $\mathrm{Sym}(\Omega)$.

In the case where Ω is finite of cardinality n, we have

$$(\mathrm{Sym}(\Omega), \Omega) \cong (\mathrm{Sym}(n), \{1, \ldots, n\}).$$

Thus, in this case, we will usually write $\mathrm{Sym}\,(\Omega) = \mathrm{Sym}\,(n) = S_n$, and say that a subgroup G of $\mathrm{Sym}(\Omega)$ is a *permutation group of degree* n.

Suppose now that G is a group acting on a set Ω, via the homomorphism $\theta : G \to \mathrm{Sym}(\Omega)$. When there is no ambiguity, we will abbreviate $\omega^{g\theta}$ to ω^g, for $g \in G$, $\omega \in \Omega$. We will also write

$$G^\Omega := G\theta, \text{ and } \mathrm{Ker}_G(\Omega) := \mathrm{Ker}(\theta)$$

to denote the image and kernel of θ, respectively. We say that G acts *faithfully* on Ω if $\mathrm{Ker}_G(\Omega) = 1$. The orbit $\omega^{G\theta}$ of $\omega \in \Omega$ under the action of G will be abbreviated to ω^G, while the stabiliser will be written as $\mathrm{Stab}_G(\omega)$. Finally, for a subset Δ of Ω, we will write $\mathrm{Stab}_G(\Delta) = \{g \in G : \Delta^g \subset \Delta\}$ for the *setwise stabiliser* of Δ in G.

As is well known, the action of G on the orbit ω^G is permutation isomorphic to the action of G on the coset space $\mathrm{Stab}_G(\omega)\backslash G$. Hence, $|\omega^G| = |G : \mathrm{Stab}_G(\omega)|$ for all $\omega \in \Omega$.

Let ω_i^G, $i \in I$, denote the orbits in Ω under the action of G (the set I is an index set). The groups $G^{\omega_i^G}$ are called the *transitive constituents* of G on Ω, and if $|I| = 1$, we say that G *acts transitively* on Ω, or G^Ω *is transitive*.

Definition 2.1.3. Let G_i, $i \in I$, be a set of groups. A subgroup G of the direct product $\prod_i G_i$ is called a *subdirect product* of the G_i if $\pi_i|_G : G \to G_i$ is surjective for each projection map $\pi_i : \prod_i G_i \to G_i$.

We note the following easily proved proposition, which will be used frequently.

Proposition 2.1.4 ([9], Theorem 1.1). *Let the group G act on the finite set Ω. Then G^Ω is isomorphic to a subdirect product of its transitive constituents.*

2.1.2 Transitive actions

In this thesis, we will be interested in transitive actions on finite sets. So assume that Ω is finite of cardinality n, and that G is a group acting transitively on Ω. In

particular, note that the action of G on Ω is permutation isomorphic to the action of G on the coset space $\mathrm{Stab}_G(\omega)\backslash G$, for any point $\omega \in \Omega$.

We now describe how the action can be "factored" into actions which are as "small" as possible.

Definition 2.1.5. Suppose that there exists a subset Δ of Ω such that:

(a) For all $g \in G$, either $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \varnothing$; and

(b) $1 < |\Delta| < n$.

Then G is said to act *imprimitively* on Ω, and G^Ω is called imprimitive. The set Δ is said to be a *block* for G (in Ω), and the set $\Delta^G = \{\Delta^g : g \in G\}$ of G-translates of Δ is called a *system of blocks* for G (in Ω). If no such subset exists, then G is said to *act primitively* on Ω, and G^Ω is called *primitive*.

We now construct the wreath product of permutation groups, as in [9]. Let R and S be permutation groups on the finite sets Δ and Γ, respectively, and let $\Omega := \Delta \times \Gamma$. We will write Ω as the union of the fibres $\Delta_\gamma := \{(\delta, \gamma) : \delta \in \Delta\}$. Now let B be the group of functions from Γ to R, with pointwise multiplication as its operation. Then B is isomorphic to the direct product of $|\Gamma|$ copies of R. The group B acts on Ω via $(\delta, \gamma)^f = (\delta^{f(\gamma)}, \gamma)$, so that each copy of R in B acts on the corresponding fibre. In particular, this action is faithful. The group S also acts on Ω, via $(\delta, \gamma)^\sigma = (\delta, \gamma^\sigma)$. Since the action of S is also faithful, we may view B and S as subgroups of $\mathrm{Sym}(\Omega)$. Furthermore, S normalises B, so we can form the semidirect product $B \rtimes S$.

Definition 2.1.6. The *(permutational) wreath product* of R and S, denoted $R \wr S$, is defined to be the semi-direct product $B \rtimes S \leq \mathrm{Sym}(\Delta \times \Gamma)$. If the set Δ is not given then we assume that $\Delta := R$, equipped with the regular action.

It will be useful to note that the action of S on B is given by $f^s(\gamma) = f(\gamma^{s^{-1}})$. For a subgroup L of R, B contains the direct product of $|\Gamma|$ copies of L: we will denote this direct product by B_L (so that $B_1 = 1$ and $B_R = B$).

Now, for each $\gamma \in \Gamma$, set

$$R_{(\gamma)} := \{f \in B : f(\gamma') = 1 \text{ for all } \gamma' \in \Gamma\backslash\{\gamma\}\} \trianglelefteq B.$$

Then $R_{(\gamma)} \cong R$, and $B = \prod_{\gamma\in\Gamma} R_{(\gamma)}$. Furthermore, $N_{R\wr S}(R_{(\gamma)}) \cong R_{(\gamma)} \times (R \wr$

$\mathrm{Stab}_S(\gamma)$). Hence, we may define the projection maps

$$\rho_\gamma : N_{R\wr S}(R_{(\gamma)}) \to R_{(\gamma)}. \tag{2.1.1}$$

We also define $\pi : R \wr S \to S$ to be the quotient map by B. This allows us to define a special class of subgroups of $R \wr S$.

Definition 2.1.7 (**[18], Definition 3).** A subgroup G of $R \wr S$ is called *large* if

(a) $N_G(R_{(\gamma)})\rho_\gamma = R_{(\gamma)}$ for all $\gamma \in \Gamma$, and;

(b) $G\pi = S$.

Remark 2.1.8. If R and S are transitive, the sets Δ and Γ each have cardinality larger than 1, and G is a large subgroup of $R \wr S$, then G is transitive, and imprimitive, with a system of blocks $\{\Delta_\gamma : \gamma \in \Gamma\}$.

In fact, it turns out that every imprimitive permutation group arises as a large subgroup of a certain wreath product.

Theorem 2.1.9 (**[48], Theorem 3.3).** *Let G be an imprimitive permutation group on a set Ω_1, and let Δ be a block for G in Ω_1. Also, let $\Gamma := \Delta^G$ be the set of G-translates of Δ, and set $\Omega_2 := \Delta \times \Gamma$. Denote by R and S the permutation groups $\mathrm{Stab}_G(\Delta)^\Delta$, and G^Γ, on Δ and Γ respectively. Then*

(i) $G \cong G^{\Omega_2}$ is isomorphic to a large subgroup of $R \wr S$, and;

(ii) (G, Ω_1) and (G, Ω_2) are permutation isomorphic.

Proof. First, let $H := \mathrm{Stab}_G(\Delta)$ and fix a right transversal $\mathcal{T}$ for H in G. Then G acts on $\mathcal{T}$ via $t^g = t.g$, where $t \in \mathcal{T}$, $g \in G$, and $t.g$ is the unique element of $\mathcal{T}$ satisfying $Htg = H(t.g)$. In particular, $tg(t.g)^{-1} \in H$. Note also that $\Gamma = \{\Delta^t : t \in \mathcal{T}\}$, since G is transitive.

Let $K_1 := \mathrm{Ker}_H(\Delta)$, and $K := \mathrm{Ker}_G(\Gamma)$. For $g \in G$, define $f_g : \Gamma \to H/K_1 \cong R$ by $f_g(\Delta^t) = K_1 tg(t.g)^{-1}$. Also, for $g \in G$, define $\alpha : G \to R \wr S$ by $g\alpha := (f_g, Kg)$. It is easy to see that α is a homomorphism. Moreover, α is injective since G acts faithfully on Ω_1. It is also easy to see that $G \cong G^\alpha \leq R \wr S$ is large.

Finally, define $\sigma : \Omega_1 \to \Omega_2$ as follows: since $\Omega_1 = \bigsqcup_{t \in \mathcal{T}} \Delta^t$, there exists, for each element $\omega \in \Omega_1$, unique elements $\delta_\omega \in \Delta$ and $t_\omega \in \mathcal{T}$ such that $\omega = \delta_\omega^{t_\omega}$. In this case, set $\sigma(\omega) := (\delta_\omega, \Delta^{t_\omega})$.

Fix $g \in G$, $\omega \in \Omega_1$ and set $h := t_\omega g (t_\omega.g)^{-1} \in H$. Since σ is a bijection by construction, and

$$\sigma(\omega^g) = \sigma(\delta_\omega^{h(t_\omega.g)}) = (\delta_\omega^h, \Delta^{t_\omega.g}) = (\delta_\omega, \Delta^{t_\omega})^{(f_g, Kg)} = (\delta_\omega, \Delta^{t_\omega})^{g\alpha},$$

the proof is complete. □

If G is an imprimitive permutation group, and the block Δ as in Theorem 2.1.9 is assumed to be a minimal block for G, then the group $R = \mathrm{Stab}_G(\Delta)^\Delta$ is primitive. When Ω_1 is finite we can iterate this process, and deduce the following.

Corollary 2.1.10. *Let G be a transitive permutation group on a finite set Ω_1. Then there exist primitive permutation groups R_1, R_2, ..., R_t such that G is a subgroup of $R_1 \wr R_2 \wr \ldots \wr R_t$.*

Remark 2.1.11. The wreath product construction is associative, in the sense that $R \wr (S \wr T) \cong (R \wr S) \wr T$, so the iterated wreath product in Corollary 2.1.10 is well-defined.

Definition 2.1.12. The tuple $(R_1, R_2, \ldots, R_t)$, where the R_i are as in Corollary 2.1.10, is called *a tuple of primitive components* for G on Ω.

We caution the reader that a tuple of primitive components for an imprimitive permutation group G on a set Ω is not necessarily unique - see [9, Page 13] for an example.

We will frequently use a result on composition length, due to Pyber. First, define the constant

$$c_0 := \log_9 48 + (1/3)\log_9 24 = 2.24399\ldots$$

We also recall the following definition from Chapter 1.

Definition 2.1.13. Let G be a finite group.

(a) Write $a(G)$ to denote the composition length of G.

(b) Let $a_{ab}(G)$ denote the number of abelian composition factors of G.

(c) Let $c_{nonab}(G)$ denote the number of nonabelian chief factors of G.

The result of Pyber can now be given as follows. It is presented in a slightly weaker form to how it is stated in [45]. As remarked in Chapter 1, its proof requires the CFSG.

Theorem 2.1.14 (**[45], Theorem 2.10).** *Let R be a primitive permutation group of degree $r \geq 2$. Then $a_{ab}(R) \leq (1 + c_0) \log r - (1/3) \log 24$, and $c_{nonab}(R) \leq \log r$.*

The stronger version [45, Theorem 2.10] of Theorem 2.1.14 gives bounds on the product of the orders of the abelian chief factors of R, which are best possible. See [45] for more details.

We shall also require the following theorem of D. Holt and C. Roney-Dougal on generator numbers in primitive groups.

Theorem 2.1.15 (**[25], Theorem 1.1).** *Let H be a subnormal subgroup of a primitive permutation group of degree r. Then $d(H) \leq \lfloor \log r \rfloor$, except that $d(H) = 2$ when $r = 3$ and $H \cong \mathrm{Sym}(3)$.*

We deduce the following easy consequence.

Corollary 2.1.16. *Let G be an imprimitive permutation group of degree n, and suppose that G has a minimal block Δ of cardinality $r \geq 4$. Let S denote the induced action of G on the set of distinct G-translates of Δ. Then $d(G) \leq s\lfloor \log r \rfloor + d(S)$, where $s := n/r$.*

Proof. Let R be the induced action of the block stabiliser $\mathrm{Stab}_G(\Delta)$ on Δ, and let $K := \mathrm{Ker}_G(\Omega)$ be the kernel of the action of G on the set Ω of distinct G-translates of Δ. Then $K^\Delta \trianglelefteq R$, and hence, by Theorem 2.1.15, each normal subgroup of K^Δ can be generated by $\lfloor \log r \rfloor$ elements.

Since $K \trianglelefteq G$, we have

$$(K, \Delta) \cong (K, \Delta^g) \tag{2.1.2}$$

for all $g \in G$. Also, since R is primitive, $K^\Delta \trianglelefteq R$ is either trivial or transitive. If K^Δ is trivial, then K is trivial by (2.1.2), and hence $d(G) = d(G/K) = d(S)$. So assume that K^Δ is transitive. Then K is a subdirect product of s copies of K^Δ, by Proposition 2.1.4. Hence, $d(K) \leq s\lfloor \log r \rfloor$ by the previous paragraph. Since $G/K \cong S$, the claim follows. □

2.2 Induced modules for finite groups

In this section, we define induced modules for finite groups, and outline some of their properties. For the remainder of the chapter, let $\mathbb{F}$ be an arbitrary field. When we say "module", we will always mean a finite dimensional right module.

Definition 2.2.1. Let G be a finite group, let H be a subgroup of G, and let V be an $\mathbb{F}[G]$-module. Then V is also an $\mathbb{F}[H]$-module, called the $\mathbb{F}[H]$-module *restricted* from the $\mathbb{F}[G]$-module V, and written $U := V\downarrow_H$.

Definition 2.2.2. Let G be a finite group, let H be a subgroup of G, and let U be an $\mathbb{F}[H]$-module. Fix a right transversal $\mathcal{T}$ for H in G, and define the $\mathbb{F}[G]$-module V by setting $V := \bigoplus_{t\in\mathcal{T}} U\otimes t$ to be the set of formal sums $v = \sum_{t\in\mathcal{T}} u\otimes t$, for $u \in U$. The action of G on V is given by $(u\otimes t)^{ht_1} = u^{h'}\otimes t'$, and extended linearly, where $tht_1 = h't'$, for t, t_1, $t' \in \mathcal{T}$, h, $h' \in H$, and $u \in U$. We write $V = U\uparrow_H^G$, and call V the $\mathbb{F}[G]$-module *induced* from the $\mathbb{F}[H]$-module U.

Remark 2.2.3. It is an easy exercise to show that, up to $\mathbb{F}[G]$-module isomorphism, the definition of $U\uparrow_H^G$ does not depend on the choice of transversal $\mathcal{T}$ for H in G.

Mackey's Theorem, which we now record, describes what happens when one restricts an induced module.

Theorem 2.2.4 (**[22], Proposition 6.20).** *Let G be a finite group, and let H and Q be subgroups of G. Let U be a finite dimensional right $\mathbb{F}[H]$-module, and let $\{x_1, x_2, \ldots, x_t\}$ be a full set of representatives for the (H, Q) double cosets in G, where t denotes the number of orbits of Q on the coset space $H\backslash G$. Then*

$$(U\uparrow_H^G)\downarrow_Q \cong \bigoplus_{i=1}^{t} U_{x_i},$$

where $U_{x_i} := (U\otimes x_i)\uparrow_{Q\cap H^{x_i}}^Q$, and $U\otimes x_i$ is the $\mathbb{F}[Q\cap H^{x_i}]$-module defined by $(u\otimes x_i)^{h^{x_i}} := u^h\otimes x_i$, where $u \in U$, $h \in H$.

We also require a well-known theorem of Frobenius, which is referred to in the literature as "Frobenius reciprosity".

Theorem 2.2.5 (**[5], Proposition 3.3.1).** *Let G be a finite group, let W be a finite dimensional right $\mathbb{F}[G]$-module, let H be a subgroup of G, and let U be a finite dimensional right $\mathbb{F}[H]$-module. Then*

$$\dim_{\mathbb{F}}\mathrm{Hom}_{\mathbb{F}[G]}(U\uparrow_H^G, W) = \dim_{\mathbb{F}}\mathrm{Hom}_{\mathbb{F}[H]}(U, W\downarrow_H).$$

We finish this section with a useful result of Alperin.

Proposition 2.2.6 (**[1], Corollary 3, Page 56).** *Let G be a finite group, and let H be a subgroup of G. If the $\mathbb{F}[G]$-module V is generated by the $\mathbb{F}[H]$-submodule U of V, and $\dim V = |G : H|\dim U$, then $V \cong U\uparrow_H^G$.*

2.3 Further results from representations

In this section we discuss some topics from the theory of representations of finite groups, which will be useful later in the thesis. We begin with Clifford's Theorem.

Theorem 2.3.1 (**[13], Theorem 49.7**). *Let G be a group, L a normal subgroup of G, and V an irreducible $\mathbb{F}[G]$-module. Then*

(i) $V\downarrow_L$ is completely reducible; and

(ii) If U is an irreducible constituent of $V\downarrow_L$, then

$$V\downarrow_L \cong e(U^{g_1}\oplus\ldots\oplus U^{g_k})$$

where $\{U^{g_1},\ldots,U^{g_k}\}$ is a full set of non-isomorphic G-conjugates of U, and e is a positive integer.

Remark 2.3.2. By $V\downarrow_L \cong e(U^{g_1}\oplus\ldots\oplus U^{g_k})$ we mean of course that $V\downarrow_L$ is isomorphic to a direct sum of e copies of the module $U^{g_1}\oplus\ldots\oplus U^{g_k}$.

Definition 2.3.3. Let G be a group, L a normal subgroup of G, and V an irreducible $\mathbb{F}[G]$-module.

(a) The submodules $e(U^{g_i})$ of $V\downarrow_L$ in Theorem 2.3.1 Part (ii) are called the *homogeneous components* of $V\downarrow_L$.

(b) If $k=1$, then $V\downarrow_L$ is said to be *homogeneous*.

Remark 2.3.4. By Theorem 2.3.1, we have $V\downarrow_L = M_1\oplus\ldots\oplus M_r$, where the $M_i\cong e(U^{g_i})$ are the homogeneous components of $V\downarrow_L$. Clearly, for $x\in G$ we have $M_i^x = M_j$ for some j, so G acts on the set $\{M_1,\ldots,M_r\}$ of homogeneous components. Furthermore, since V is irreducible, this action is transitive.

Remark 2.3.5. Let G be a group, and V an n-dimensional $\mathbb{F}[G]$-module. Let $\mathbb{K}$ be an extension field of $\mathbb{F}$. Then the $\mathbb{F}[G]$-representation $\rho: G\to GL_n(\mathbb{F})$ associated to V can be viewed as a $\mathbb{K}[G]$-representation, just by viewing the matrix as having entries in $\mathbb{K}$; we write this $\mathbb{K}[G]$-representation as $\rho^{\mathbb{K}}$ (this merely indicates a change in point of view). In module theoretic language, the $\mathbb{K}[G]$-module associated to $\rho^{\mathbb{K}}$ is $V\otimes_{\mathbb{F}}\mathbb{K}$, and will be denoted by $V^{\mathbb{K}}$. In the literature, the module $V^{\mathbb{K}}$ is sometimes refereed to as an *extension of scalars* of V to $\mathbb{K}$. Note also that $\dim_{\mathbb{K}}(V^{\mathbb{K}}) = \dim_{\mathbb{F}}(V)$.

We now record two lemmas which will be key in the proof of Proposition 5.3.7. The first has a stronger version which is stated in [25, Lemma 2.13], but we only require the following.

Lemma 2.3.6 ([25], Lemma 2.13). *Let $G \leq GL_n(\mathbb{F})$ be finite, let $V = \mathbb{F}^n$ be the natural module, and assume that G acts irreducibly on V. Suppose that*

1. *$V\downarrow_L$ is homogeneous for each normal subgroup L of G; and*
2. *G has no non-trivial abelian quotients.*

Then G is isomorphic to a subgroup of $GL_{n/f}(\mathbb{K})$ for some divisor f of n, and some extension field $\mathbb{K}$ of $\mathbb{F}$ of degree f. Furthermore, if W denotes the natural module for $GL_{n/f}(\mathbb{K})$, then G acts irreducibly on W and

(i) $W\downarrow_L$ is homogeneous for each normal subgroup L of G;

(ii) $Z(G)$ is cyclic; and

(iii) Each abelian characteristic subgroup of G is contained in $Z(GL_{n/f}(\mathbb{K}))$.

Lemma 2.3.7. *Let $G \leq GL_n(\mathbb{F})$ be finite, let V be the natural module, and assume that V is irreducible. Suppose that $1 \neq E \trianglelefteq L \trianglelefteq G$, and that $V\downarrow_L$ is homogeneous. Suppose that $\mathbb{K} \supseteq \mathbb{F}$ is a splitting field for all subgroups of L, and assume that the resulting extension $\mathbb{K}/\mathbb{F}$ is normal. Then $V^{\mathbb{K}}\downarrow_E$ is a non-trivial completely reducible $\mathbb{K}[E]$-module.*

Proof. Since L is homogeneous, $V\downarrow_L \cong eU$, for some irreducible $\mathbb{F}[L]$-module U and some positive integer e. Since G is faithful on V and $L \neq 1$, L is faithful on U. Moreover, $U^{\mathbb{K}}$ is completely reducible, and each of its irreducible constituents are algebraically conjugate, by [13, Theorem 70.15]. It follows that L is faithful on $V^{\mathbb{K}}\downarrow_L$, and hence $V^{\mathbb{K}}\downarrow_E$ is non-trivial. Also, since $E \trianglelefteq L$, and

$$V^{\mathbb{K}}\downarrow_E \cong V^{\mathbb{K}}\downarrow_L\downarrow_E,$$

it follows from Theorem 2.3.1 that $V^{\mathbb{K}}\downarrow_E$ is completely reducible. This completes the proof. □

Remark 2.3.8. Let $\mathbb{K}$ be a splitting field for the finite group G, containing the field $\mathbb{F}$. Then every field $\mathbb{E}$ containing $\mathbb{K}$ is also a splitting field for G (for example, see [27, Corollary 9.8]). Thus, one can always find a splitting field $\mathbb{E}$ for G such that $\mathbb{E}/\mathbb{F}$ is a normal extension (for instance, by taking $\mathbb{E}$ to be the normal closure of $\mathbb{K}/\mathbb{F}$).

2.4 Number Theory: The prime counting function

We close this chapter with a brief discussion of large prime power divisors of positive integers.

Definition 2.4.1. For a positive integer s and a prime p, write s_p for the p-part of s. Also, define $\operatorname{lpp} s = \max_{p \text{ prime}} s_p$ to be the largest prime power divisor of s.

Fix $s \geq 2$, and let $k = \operatorname{lpp} s$. By writing the prime factorization of s as $s = kp_2^{r_2} \dots p_t^{r_t}$, one immediately sees that $s \leq k^{\delta(k)}$, where $\delta(k)$ denotes the number of primes less than or equal to k. Hence, $\log s \leq \delta(k) \log k$. Also, it is proved in [46, Corollary 1] that

$$\delta(k) < 1.25506k/\ln k$$

for $k \geq 2$. Define the constant c' by

$$c' := \ln 2/1.25506 \tag{2.4.1}$$

We deduce the following.

Lemma 2.4.2. *Let s be a positive integer. Then*

$$\operatorname{lpp} s \geq (\ln 2/1.25506) \log s = c' \log s.$$

Part I

Generating minimally transitive groups

Chapter 3

Generating minimally transitive permutation groups

3.1 Introduction

We begin this chapter with a definition.

Definition 3.1.1. A transitive permutation group G is said to be *minimally transitive* if every proper subgroup of G is intransitive.

For example, a finite group G acting on itself by right multiplication (i.e. the regular action) is minimally transitive of degree $|G|$. Another example includes the alternating group $G := \mathrm{Alt}(5)$. Of course, G is not minimally transitive in its natural action on 5 points (a cyclic subgroup of order 5 is transitive, for example), but G does acts minimally transitively on the cosets of a subgroup of order 3 (or a subgroup of order 4).

Apart from their independent interest, minimally transitive groups have applications in Combinatorics (for counting vertex transitive graphs; for example, see [4]), and in the theory of BFC-groups (see [42] and [47]). In Chapter 4, we study the structure of minimally transitive groups of degree $2^m 3$, and later on in the thesis we use the results therein to study minimal generator numbers in modules for permutation groups.

In this chapter, we consider the minimal number of elements required to generate such a group, in terms of its degree n. For the prime factorisation $n = \prod_{p \text{ prime}} p^{n(p)}$ of n, recall from Definition 1.3.2 that $\omega(n) := \sum_p n(p)$. We will also define $\mu(n) := \max\{n(p) : p \text{ prime}\}$.

Motivated by the problem of bounding the order of the derived subgroup of a BFC-group, the question of bounding $d(G)$ in terms of n was first considered by Shepperd and Wiegold in [47]. There, they prove that every minimally transitive group of degree n can be generated by $\omega(n)$ elements. It was then suggested by Pyber (see [45]) to investigate whether or not $\mu(n)+1$ elements would always suffice. A. Lucchini gave a partial answer to this question in [34], proving that: *if G is a minimally transitive group of degree n, and $\mu(n)+1$ elements are not sufficient to generate G, then $\omega(n) \geq 2$ and $d(G) \leq \lfloor \log_2(\omega(n)-1)+3 \rfloor$.*

In this chapter, we offer a complete solution to the problem, proving

Theorem 1.2.1. *Let G be a minimally transitive permutation group of degree n. Then $d(G) \leq \mu(n)+1$.*

If p is an odd prime, and $G := (C_p)^n \rtimes C_2$, with the generator in C_2 acting by inverting the non-identity elements in $(C_p)^n$, then $d(G) = n+1 = \mu(|G|)+1$, so the bound in Theorem 1.2.1 is best possible.

Our approach follows along the same lines as Lucchini's proof of the main theorem in [34]. Indeed, his methods suffice to prove Theorem 1.2.1 in the case when a minimal normal subgroup of a "crown" for G is abelian (see Section 3.3). Thus, our main efforts will be concerned with the case when a minimal normal subgroup of a crown for G is a direct product of isomorphic non-abelian simple groups. The key step in this direction is Lemma 3.4.1, which we prove in Section 3.4. We use Section 3.3 to outline the method of *crown-based powers* due to F. Dalla Volta and Lucchini [14]; this will serve as the basis for our arguments. Section 3.2 is reserved for a preliminary lemma on minimally transitive groups, which will also be used in Chapter 4. Finally, we prove Theorem 1.2.1 in Section 3.5.

3.2 Some observations on minimally transitive groups

We begin preparations towards the proof of Theorem 1.2.1 with some easy observations on minimally transitive groups.

Lemma 3.2.1. *Let G be a transitive subgroup of S_n, let A be a point stabiliser in G, let $1 \neq L$ be a normal subgroup of G, and let $\Omega = \{\Delta_1, \ldots, \Delta_t\}$ be the set of L-orbits. Then*

(i) Either L is transitive, or Ω forms a system of blocks for G. In particular, the size of an L-orbit divides n.

(ii) (L, Δ_1) *is permutation isomorphic to* (L, Δ_j)*, for all* j*.*

(iii) $|\Omega| = |G : AL|$*.*

(iv) G *is minimally transitive if and only if the only subgroup* $X \leq G$ *satisfying* $AX = G$ *is* $X = G$*.*

(v) If G *is minimally transitive, then* G^Ω *is minimally transitive.*

(vi) If $n = p^a$ *for a prime* p *and* G *is minimally transitive, then* G *is a* p*-group.*

Proof. Part (i) is clear, so we prove (ii): Fix j in the range $1 \leq j \leq t$. By (i), there exists $g \in G$ such that $\Delta_1^g = \Delta_j$. Let $\alpha_g : L \to L$ denote the automorphism of L induced by conjugation by g, and define $\sigma : \Delta_1 \to \Delta_j$ by $\sigma(\delta) = \delta^g$, for $\delta \in \Delta_1$. Then

$$\sigma(\delta^l) = \delta^{lg} = \sigma(\delta)^{l^g} = \sigma(\delta)^{(l\alpha_g)},$$

for $l \in L$, $\delta \in \Delta_1$. This proves (ii).

If L is transitive, then $AL = G$, so $|\Omega| = 1 = |G : AL|$. Otherwise, Part (i) implies that the size of each L-orbit is $|L : L \cap A| = |AL : A|$, so the number of L-orbits is $n/|AL : A| = |G : AL|$. Part (iii) follows.

Now, a subgroup X of G is transitive if and only if $AX = G$. Hence, Part (iv) follows.

Part (v) is proved in [15, Theorem 2.4]. Finally, Part (vi) follows since a Sylow p-subgroup of a transitive group of degree p^a acts transitively. □

3.3 Crown-based powers

In this section, we outline an approach to study the question of finding the minimal number of elements required to generate a finite group, which is due to F. Dalla Volta and A. Lucchini. So let G be a finite group, with $d(G) = d > 2$, and let M be a normal subgroup of G, maximal with the property that $d(G/M) = d$. Then G/M needs more generators than any proper quotient of G/M, and hence, as we shall see below, G/M has a very restrictive structure. We remark that G/M is sometimes referred to in the literature as a *crown* for G.

We describe this structure as follows: let L be a finite group, with a unique minimal normal subgroup N. If N is abelian, then assume further that N is complemented in L. Now, for a positive integer k, set L_k to be the subgroup

of the direct product L^k defined as follows

$$L_k := \{(x_1, x_2, \ldots, x_k) : x_i \in L,\ Nx_i = Nx_j \text{ for all } i, j\}$$

Equivalently, $L_k := \mathrm{diag}(L^k)N^k$, where $\mathrm{diag}\,(L^k)$ denotes the diagonal subgroup of L^k. The group L_k is called the *crown-based power of L of size k*. Note that $\mathrm{Soc}(L_k) = N^k$.

We can now state the theorem of Dalla Volta and Lucchini.

Theorem 3.3.1 (**[14], Theorem 1.4**). *Let G be a finite group, with $d(G) \geq 3$, which requires more generators than any of its proper quotients. Then there exists a finite group L, with a unique minimal normal subgroup N, which is either nonabelian or complemented in L, and a positive integer $k \geq 2$, such that $G \cong L_k$.*

Remark 3.3.2. It is clear that, for fixed L, $d(L_k)$ increases with k. Indeed, if we identify L with the first coordinate subgroup of L^k, then $L_k \cap L \cong N$, and $L_k/(L \cap L_k) \cong L_{k-1}$.

To use Theorem 3.3.1, we will need a bound on $d(L_k)$, in terms of k. This is provided by the next two results. Before giving the statements, we require some additional notation: let d be a positive integer. For a finite group G, let $\phi_G(d)$ denote the number of ordered d-tuples of elements of G which generate G. Now, set

$$P_G(d) := \frac{\phi_G(d)}{|G|^d}$$

so that $P_G(d)$ denotes the probability that d randomly chosen elements of G generate G. Finally, for a normal subgroup M of G, define

$$P_{G,M}(d) := \frac{P_G(d)}{P_{G/M}(d)}.$$

$P_{G,M}(d)$ represents the conditional probability that d randomly chosen elements of G generate G, given that their images modulo M generate G/M.

Remark 3.3.3. If L is a finite group with a unique minimal normal subgroup N, then $C_L(N) = Z(N)$. Thus, $L/Z(N)$ can be embedded as a subgroup of $\mathrm{Aut}(N)$. Hence, since $(L/Z(N))/(N/Z(N)) \cong L/N$, and $N/Z(N) \cong \mathrm{Inn}(N) \trianglelefteq \mathrm{Aut}(N)$, the group $C_{\mathrm{Aut}(N)}(L/N)$ is well-defined.

Theorem 3.3.4 (**[34], Theorem 2.1 and [14], Theorem 2.7**). *Let L be a finite group with a unique minimal normal subgroup N which is either nonabelian or*

complemented in L, and let k be a positive integer. Assume also that $d(L) \leq d$. Then

(i) If N is abelian, then $d(L_k) \leq \max\{d(L), k+1\}$;

(ii) If N is nonabelian, then $d(L_k) \leq d$ if and only if $k \leq P_{L,N}(d)|N|^d/|C_{\mathrm{Aut}\,(N)}(L/N)|$.

Proof. Part (i) follows immediately from [34, Theorem 2.1], so we just prove (ii). So assume that N is nonabelian. By Remark 3.3.2 above, $d(L_k)$ increases with k. Thus, since $d \geq d(L) = d(L_1)$, there exists a largest positive integer $f_L(d)$ such that $d(L_{f_L(d)}) \leq d$. Furthermore, by [14, Theorem 2.7], we have

$$f_L(d) = \frac{\phi_L(d)}{|C_{\mathrm{Aut}\,(N)}(L/N)|\phi_{L/N}(d)}.$$

Since

$$P_{L,N}(d) = \frac{P_L(d)}{P_{L/N}(d)} = \frac{\phi_L(d)}{\phi_{L/N}(d)|N|^d}$$

the result follows. □

We will also need an estimate for $P_{L,N}(d)$.

Theorem 3.3.5 (**[17], Theorem 1.1**). *Let L be a finite group, with a unique minimal normal subgroup N, which is nonabelian, and suppose that $d \geq d(L)$. Then $P_{L,N}(d) \geq 53/90$.*

3.4 Indices of proper subgroups in finite simple groups

For a positive integer m, $\pi(m)$ denotes the set of prime divisors of m.

Lemma 3.4.1. *Let S be a nonabelian simple group. Then there exists a set of primes $\Gamma = \Gamma(S)$ with the following properties:*

(i) $|\Gamma| \leq f(S)$, where $f(S) := r/2 + 1$ if S is an alternating group of degree r, and $f(S) := 4$ otherwise;

(ii) $\pi(|S : H|)$ intersects Γ nontrivially for every proper subgroup H of S.

Proof. If $S = L_2(p)$, for some prime p, then since every maximal subgroup M of S has index divisible by either p or $p+1$ (see [19], for example), we can take $\Gamma(S) = \{2, p\}$. If $S = L_2(8)$, $L_3(3)$, $U_3(3)$ or $\mathrm{Sp}_4(8)$, then direct computation using

MAGMA (or Tables 8.1 to 8.6 and Table 8.14 in [7]), implies that each maximal subgroup of S has index divisible by at least one of the primes in $\{2,3\}$, $\{2,13\}$, $\{3,7\}$, and $\{2,3\}$, respectively.

Next, assume that $S = A_r$ is an alternating group of degree r, and let p and q be the two largest primes not exceeding r, where $p > q$. If $r = p$, then we can take $\Gamma := \{r, q\}$, by [30, Theorem 4]. So assume that $p < r$, and for each k in $p \leq k \leq r-1$, choose a prime divisor q_k of $\binom{r}{k}$. Then set $\Gamma := \Gamma(A_r) = \{q_p, \ldots, q_{r-1}\} \cup \{p, q\}$. We claim that Γ satisfies (i) and (ii). To see this, note that $|\Gamma| \leq r - p + 2$, which is less than $r/2 + 2$ by Bertrand's postulate. This proves (i). To see that (ii) holds, let H be a proper subgroup of A_r. If p or q does not divide $|H|$ then we are done, so assume that pq divides $|H|$. Then $A_k \trianglelefteq H \leq S_k \times S_{r-k}$, for some k with $p \leq k \leq r-1$, by [30, Theorem 4]. Hence, H has index divisible by $\binom{r}{k}$, and (ii) follows.

So assume that S is not one of the simple groups considered in the first two paragraphs above, and let $\Pi = \Pi(S)$ be the set of prime divisors of $|S|$ discussed in [30, Corollary 6], so that $|\Pi| \leq 3$. If S does not occur in the left hand column of Table 10.7 in [30], then $\Gamma := \Pi$ satisfies the conclusion of the lemma, by [30, Corollary 6], so assume otherwise.

Then S is one of the simple groups in the first column of [30, Table 10.7]; we need to prove that there exists a set Γ as in the statement of the lemma. If $H < S$ is not one of the exceptions listed in the middle column of Table 10.7, then $|S : H|$ intersects Π non-trivially. Thus, all we need to prove is that there exists a prime p such that, whenever H is one of these exceptional subgroups, then p divides $|S : H|$. Indeed, in this case, $\Gamma := \Pi \cup \{p\}$ gives us what we need.

So let H be one of these subgroups. We consider each of the possibilities from [30, Table 10.7]:

1. Suppose that either

   (a) $S = \mathrm{PSp}_{2m}(q)$ (m, q even) or $\mathrm{P}\,\Omega_{2m+1}(q)$ (m even, q odd), and $\Omega^-_{2m}(q) \trianglelefteq H$; or

   (b) $S = \mathrm{P}\,\Omega^+_{2m}(q)$ (m even, q odd), and $\Omega_{2m-1}(q) \trianglelefteq H$; or

   (c) $S = \mathrm{PSp}_4(q)$ and $\mathrm{PSp}_2(q^2) \trianglelefteq H$.

   Let p be the defining characteristic of S. Since H is not a parabolic subgroup of G, H does not contain a Sylow p-subgroup of S. Hence, our choice of p gives us what we need.

2. In each of the remaining cases (see [29, Table 10.7]), we are given a tuple (S, Y_1,..., $Y_{t(S)}$), where $t(S) \leq 4$, S is one of $L_2(8)$, $L_3(3)$, $L_6(2)$, $U_3(3)$, $U_3(3)$, $U_3(5)$, $U_4(2)$, $U_4(3)$, $U_5(2)$, $U_6(2)$, $\mathrm{PSp}_4(7)$, $\mathrm{PSp}_4(8)$, $\mathrm{PSp}_6(2)$, $\mathrm{P}\,\Omega_8^+(2)$, $G_2(3)$, ${}^2F_4(2)'$, M_{11}, M_{12}, M_{24}, HS, McL, Co_2 or Co_3, $Y_i < S$ for each $1 \leq i \leq t(S)$, and H is contained in at least one of the groups Y_i. In each case, we can easily see that there is a prime p, with p dividing $|S : Y_i|$ for each i in $1 \leq i \leq t(S)$.

This completes the proof. □

3.5 The proof of Theorem 1.2.1

Recall that for a group G acting on a set Ω, we write G^Ω for the image of the induced action of G on Ω. Before proceeding to the proof of Theorem 1.2.1, we need two lemmas.

Lemma 3.5.1 ([38], Proof of Lemma 3). *Let L be a finite group with a unique minimal normal subgroup N, which is nonabelian, and write $N \cong S^t$, where S is a nonabelian simple group. Then $|C_{\mathrm{Aut}\,(N)}(L/N)| \leq t|S|^t|\,\mathrm{Out}\,(S)|$.*

Lemma 3.5.2 ([31], Proposition 4.4). *Let S be a nonabelian finite simple group. Then $|\,\mathrm{Out}\,(S)| \leq |S|^{1/4}$.*

The preparations are now complete.

Proof of Theorem 1.2.1. Assume that the theorem is false, and let G be a counterexample of minimal degree. Also, let A be the stabiliser in G of a point α, and let $m := \mu(n) + 1$.

First, we claim that G needs more generators than any proper quotient of G. To this end, let M be a non-trivial normal subgroup of G, and let K be the kernel of the action of G on the set of M-orbits. Then G/K is minimally transitive of degree $s := |G : AM|$, by Lemma 3.2.1 Parts (iii) and (v), and hence, since s divides n, the minimality of n implies that there exists elements x_1, x_2, ..., x_m in G such that $G = \langle x_1, x_2, \ldots, x_m, K\rangle$. But then $H := \langle x_1, x_2, \ldots, x_m\rangle$ acts transitively on the set of M-orbits, so $HM = G$ by minimal transitivity of G. Hence $d(G/M) \leq m$, which proves the claim.

Hence, by Theorem 3.3.1, $G \cong L_k$, for some $k \geq 2$, and some group L with a unique minimal normal subgroup N, which is either nonabelian, or complemented in L. We now fix some notation: write $\mathrm{Soc}\,(G) = N_1 \times N_2 \times \ldots \times N_k$, where each

$N_i \cong N \cong S^t$, for some simple group S, and $t \geq 1$, and set $X_i := N_1 \times N_2 \times \ldots \times N_i$. We will also write $X_0 := 1$, $H_{i+1} = N_{i+1} \cap X_i A$, and we denote by Δ_i the X_i-orbit containing α, for $0 \leq i \leq k$. Then $|\Delta_i| = n|X_i A|/|G|$ by Lemma 3.2.1 Part (iii), and hence

$$\frac{|\Delta_{i+1}|}{|\Delta_i|} = \frac{|X_{i+1}A|}{|X_i A|} = \frac{|N_{i+1}X_i A|}{|X_i A|} = |N_{i+1} : H_{i+1}|$$

Furthermore, it is shown in the proof of the main theorem in [34], that $|\Delta_{i+1}|/|\Delta_i| = |N_{i+1} : H_{i+1}|$ is greater than 1 for $0 \leq i \leq k-2$, and also for $i = k-1$ if N is abelian. Note also that $G/\operatorname{Soc}(G) \cong L/N$ is m-generated, by the previous paragraph; thus, L is m-generated (see Theorem 6.2.2).

We now separate the cases of N being abelian or nonabelian. If N is abelian, then $N \cong C_p^t$, for some prime p, so by the previous paragraph, p divides $|N_{i+1} : H_{i+1}| = |\Delta_{i+1}|/|\Delta_i|$ for each $0 \leq i \leq k-1$. Thus, p^k divides $|\Delta_k|$, and hence divides n, by Lemma 3.2.1 Part (i). It follows that $k \leq \mu(n)$, which, by Theorem 3.3.4 Part (i), contradicts our assumption that $d(G) > \mu(n) + 1$.

Thus, N is nonabelian. Hence, by the third paragraph, for each i in $0 \leq i \leq k-2$, N_{i+1} has a direct factor S_{i+1} ($S_{i+1} \cong S$), with $|S_{i+1} : S_{i+1} \cap H_{i+1}| > 1$. Let $\Gamma = \Gamma(S)$ be the set of primes in Lemma 3.4.1, so that $|\Gamma| \leq f(S)$, where $f(S)$ is as defined in Lemma 3.4.1. Then Lemma 3.4.1 implies that for each $0 \leq i \leq k-2$, the index $|S_{i+1} : S_{i+1} \cap H_{i+1}|$, and hence $|\Delta_{i+1}|/|\Delta_i| = |N_{i+1} : H_{i+1}|$, is divisible by some prime p_{i+1} in Γ.

So we now have a list of primes $p_1, p_2, \ldots, p_{k-1}$, with each p_i in Γ, such that the product $\prod_{i=1}^{k-1} p_i$ divides $|\Delta_{k-1}|$. For each prime p in Γ, let $a_{(p)}$ be the number of times that p occurs in this product. Then, since $|\Delta_{k-1}|$ divides n by Lemma 3.2.1 Part (i), $\prod_{p\in\Gamma} p^{a_{(p)}}$ divides n. Since $|\Gamma| \leq f(S)$, and $\sum_{p\in\Gamma} a_{(p)} = k-1$, we have $a_{(p)} \geq (k-1)/f(S)$ for at least one prime p in Γ. Hence, $(k-1)/f(S) \leq \mu(n)$, and it follows that

$$k \leq f(S)\mu(n) + 1 \leq \frac{53|S|^{t\mu(n)}}{90t|\operatorname{Out}(S)|} \qquad \text{(see the paragraph below)} \qquad (3.5.1)$$

$$\leq \frac{53|N|^m}{90|C_{\operatorname{Aut}(N)}(L/N)|} \qquad \text{(by Lemma 3.5.1)} \qquad (3.5.2)$$

$$\leq \frac{P_{L,N}(m)|N|^m}{|C_{\operatorname{Aut}(N)}(L/N)|} \qquad \text{(by Theorem 3.3.5)} \qquad (3.5.3)$$

Note that $|N| = |S|^t$. Then the inequality in (3.5.1) above follows easily when S is an alternating group of degree r, since $|S| = r!/2$, and $|\operatorname{Out}(S)| \leq 4$ in this case

(also, $|\operatorname{Out}(S)| \leq 2$ if $r \neq 6$). It also follows easily when S is not an alternating group, using Lemma 3.5.2. Now, by Theorem 3.3.4 Part (ii), the inequality in (3.5.3) contradicts our assumption that $d(G) > m$. This completes the proof. $\square$

Part II

Generating transitive groups

Chapter 4

Minimally transitive groups of degree $2^m 3$

4.1 Introduction

We begin the second part of this thesis with a continuation of our discussion of minimally transitive permutation groups. As mentioned in Chapter 3, we use these groups in Part II to study minimal generator numbers in modules for permutation groups. Specifically, as mentioned in Chapter 1, if $H \leq G$ are finite groups, V is a G-module, and $\widetilde{G}$ is a subgroup of G acting transitively on the set $H\backslash G$ of right cosets of H in G, then $V\uparrow_H^G \cong V\uparrow^{\widetilde{G}}_{\widetilde{G}\cap H}$, by Theorem 2.2.4. Thus, when studying induced modules, one may often reduce to the case where G acts minimally transitively on $H\backslash G$.

Note also that the bounds we obtain in Theorem 5.4.15 and its corollaries are strong enough to prove Theorem 6.1.3 in most cases. Due to the nature of the bounds however, this is not the case when $|G : H|$ has the form $2^m 3$. Thus, we have to work harder, and try to obtain some information about the structure of the minimally transitive groups of degree $2^m 3$. Recall from Chapter 1 that our main result is as follows.

Theorem 1.2.4. *Let G be a minimally transitive permutation group of degree $n = 2^m 3$. Then one of the following holds:*

(i) G is soluble; or

(ii) G has a unique nonabelian chief factor, which is a direct product of copies of $L_2(p)$, where p is a Mersenne prime.

A minimally transitive group of prime power degree is a p-group (see Lemma 3.2.1), and therefore soluble. Therefore, another motivation behind Theorem 1.2.4 is to study how far away from being soluble a minimally transitive group of degree $n := 2^m 3$ is. It would be interesting to study the same question for minimally transitive groups of degree $n := p^m q$, for arbitrary primes p and q. For an analysis of the case $n = pq$, for distinct primes p and q, see [15].

4.2 Subgroups of index $2^m 3$ in direct products of nonabelian simple groups

In [30, Corollary 6], information is given regarding the prime divisors of indices of subgroups of simple groups. We utilise this work for the second time in this thesis in the following proposition.

Proposition 4.2.1. *Let T be a nonabelian finite simple group, and suppose that T has a proper subgroup X of index $n = 2^i 3^j$, with $0 \leq j \leq 1$. Then one of the following holds:*

(i) $T = M_{12}$ and X is contained in one of the two T-conjugacy classes of copies of M_{11} in M_{12}.

(ii) $T = M_{11}$ or M_{24}, and X is T-conjugate to $L_2(11)$ or M_{23}, respectively.

(iii) $T = A_r$, $r = 2^i 3^j$, and either X is T-conjugate to A_{r-1}, or $r = 6$ and X is T-conjugate to $L_2(5)$.

(iv) $T = L_2(p)$ where p is a prime of the form $p = 2^{f_1} 3^{f_2} - 1$ with $f_2 \leq 1$, and X is a subgroup of index either 1 or 3 in a T-conjugate of the maximal subgroup $M = C_p \rtimes C_{(p-1)/2} < L_2(p)$.

Proof. For a finite set F, let $\pi(F)$ denote the set of prime divisors of $|F|$. Thus, we have $\pi(X) \subseteq \pi(T)$, since $X \leq T$. We wish to reduce to the case $\pi(X) = \pi(T)$ and then use [30, Corollary 6]. However, we first need to deal with some cases which are not covered by this approach. First, the classification of the maximal subgroups of the simple classical groups of dimension up to 12 implies that T is not $L_2(8)$, $L_3(3)$, $U_3(3)$, $\mathrm{Sp}_4(8)$, $U_4(2)$ or $U_5(2)$ (see [7, Tables 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.10, 8.11, 8.14, 8.20 and 8.21]).

Assume next that $T \cong L_2(p)$, for some prime p of the form $p = 2^{f_1} 3^{f_2} - 1$, with $f_2 \geq 0$. Also, let M be a maximal subgroup of T containing X. Then, since

$|T : M|$ divides $|T : X| = 2^i 3^j$ with $j \leq 1$, we must have $M = C_p \rtimes C_{(p-1)/2}$, and $f_2 \leq 1$ (see [7, Table 8.1]). Set $l := 1$ if $f_2 = 0$, and $l := 3$ if $f_2 = 1$. Since $(p+1)/l$ is the highest power of 2 dividing $|T|$, and $|T : X| = 2^i 3^j$ with $j \leq 1$, either $X = M$; or $f_2 = 0$ and $|M : X| = 3$. This is the situation described in (iv).

Next, assume that T is one of the Mathieu groups M_{11} or M_{12}. Using the $\mathbb{ATLAS}$ [12], we find that the only possibilities for X are $T = M_{11}$ and X is T-conjugate to $L_2(11) \leq M_{11}$ (of index 12); or $T = M_{12}$ and X is a member of one of the two T-conjugacy classes of $M_{11} \leq M_{12}$ (of index 12).

Finally, assume that T is not one of the groups considered above, and let Π be the set of primes for T given in the statement of [30, Corollary 6]. Then $\pi(|T : X|) \subseteq \{2, 3\}$, and $q \geq 5$ for each $q \in \Pi$ (the cases where Π contains 2 or 3 have been dealt with in the preceding paragraphs - see [30, Corollary 6]). Thus, we must have $\Pi \subseteq \pi(X)$. Hence [30, Corollary 6] gives $\pi(X) = \pi(T)$ and the possibilities for T and X are as follows (see [30, Table 10.7]).

(1) $T = A_r$, $A_k \trianglelefteq X \leq S_k \times S_{r-k}$, and k is greater than or equal to the largest prime p with $p \leq r$ (in particular, $k \geq 5$, since T is simple). Then $|A_r : A_r \cap (S_k \times S_{r-k})| = \binom{r}{k}$ divides $|T : X| = 2^i 3^j$. But a well-known theorem of Sylvester and Schur (see [23]) states that either $\binom{r}{k} = 1$ or $\binom{r}{k}$ has a prime divisor exceeding $\min\{k, r-k\}$. Thus, since $k \geq 5$ we must have $k = r-2$ or $k = r-1$. Since $r \geq 5$, $k = r-1$ is the only option and hence $X = A_{r-1}$, which gives us what we need.

(2) $T = A_6$, $X = L_2(5)$. This, together with (1) above, gives precisely the situation described in (iii).

(3) $T = \mathrm{PSp}_{2m}(q)$ (m, q even) or $\mathrm{P}\,\Omega_{2m+1}(q)$ (m even, q odd), and $\Omega^-_{2m}(q) \trianglelefteq X$. Then $X \leq N_T(\Omega^-_{2m}(q))$, so $|T : N_T(\Omega^-_{2m}(q))|$ divides $|T : X| = 2^i 3^j$. But $|N_T(\Omega^-_{2m}(q)) : \Omega^-_{2m}(q)| = 2$, by [29, Proposition 4.8.6] for $T = \mathrm{PSp}_{2m}(q)$ and [29, Proposition 4.1.6] for $T = \mathrm{P}\,\Omega_{2m+1}(q)$. Hence, $|T : \Omega^-_{2m}(q)|$ divides $2^{i+1}3^j$. Also, for each of the two choices of T we get $|T : \Omega^-_{2m}(q)| = q^m(q^m - 1)$. But $q^m(q^m - 1)$ cannot be of the form 2^f or $2^f 3$, since $m > 1$ and $(m, q) \neq (2, 2)$ (as T is simple). Therefore, we have a contradiction.

(4) $T = \mathrm{P}\,\Omega^+_{2m}(q)$ (m even, q odd) and $\Omega_{2m-1}(q) \trianglelefteq X$. As above, $X \leq N_T(\Omega_{2m-1}(q))$, and we use [29, Proposition 4.1.6 Part (i)] to conclude that $|N_T(\Omega_{2m-1}(q)) : \Omega_{2m-1}(q)| = 2$. It follows that $\frac{1}{2}q^{m-1}(q^m - 1) = |T : \Omega_{2m-1}(q)|$ divides $2^{i+1}3^j$. This again gives a contradiction, since $m \geq 4$.

(5) $T = \mathrm{PSp}_4(q)$ and $\mathrm{PSp}_2(q^2) \trianglelefteq X$. Then $X \leq N_T(\mathrm{PSp}_2(q^2))$, and [29, Proposition 4.3.10] gives $|N_T(\mathrm{PSp}_2(q^2)) : \mathrm{PSp}_2(q^2)| = 2$. It follows that $q^2(q^2-1) = |T : \mathrm{PSp}_2(q^2)|$ divides $2^{i+1}3^j$. Again, this is impossible.

(6) In each of the remaining cases (see [29, Table 10.7]), we are given a pair (T, Y), where T is $L_2(8)$, $L_3(3)$, $L_6(2)$, $U_3(3)$, $U_3(5)$, $U_4(3)$, $U_6(2)$, $\mathrm{PSp}_4(7)$, $\mathrm{PSp}_4(8)$, $\mathrm{PSp}_6(2)$, $\mathrm{P}\,\Omega_8^+(2)$, $G_2(3)$, ${}^2F_4(2)'$, M_{24}, HS, McL, Co_2 or Co_3, and Y is a subgroup of T containing X. Apart from when $T = M_{24}$, we find that $|T : Y|$ does not divide 2^i3^j, so we get a contradiction in each case. When $T = M_{24}$, the only possibility is when X is T-conjugate to $M_{23} \leq M_{24}$ (of index 24).

This completes the proof. □

Our main tool in proving Theorem 1.2.4 is the Frattini argument. The result is well-known, but we couldn't find a reference so we include a proof here.

Lemma 4.2.2. *Let G be a group, and let L be a normal subgroup of G. Suppose that H is a subgroup of L with the property that H and H^α are L-conjugate for each $\alpha \in \mathrm{Aut}(L)$. Then $G = N_G(H)L$.*

Proof. Let $g \in G$. Then conjugation by g induces an automorphism of L, so $H^g = H^l$ for some $l \in L$, by hypothesis. Hence, $gl^{-1} \in N_G(H)$, so $g \in N_G(H)L$, and this completes the proof. □

With the Frattini argument in mind, the next corollary will be crucial.

Lemma 4.2.3. *Let T be a nonabelian finite simple group, and suppose that T has a proper subgroup X of index $r := 2^i3^j$, with $0 \leq j \leq 1$. Assume also that if $T \cong L_2(p)$, with p a Mersenne prime, then $j = 0$. Denote by Γ the set of right cosets of X in T. Then there exists a proper subgroup H of T with the following properties:*

(i) H and H^α are conjugate in T for each automorphism $\alpha \in \mathrm{Aut}(T)$; and

(ii) $N_T(H)^\Gamma$ is transitive.

Proof. By Proposition 4.2.1, the possibilities for the pair (T, X) (up to conjugation in T) are as follows:

1. $(T, X) = (A_r, A_{r-1})$, with $r = 2^i3^j$ for some $j \leq 1$, or $(T, X) = (A_6, L_2(5))$. Since T is nonabelian simple, $r \geq 6$, so r is even. If r is a power of 2, let H

be a Sylow 2-subgroup of T. Then H^Γ itself is transitive, and properties (i) and (ii) are clearly satisfied.

Otherwise, let $H = \langle (1,2,3), (4,5,6), \ldots, (r-1, r-2, r) \rangle$. Then $N_T(H)^\Gamma$ is transitive. Thus, (ii) is satisfied. Property (i) is also easily seen to be satisfied (this includes the case $r = 6$, when $\mathrm{Out}\,(A_6)$ has order 4).

2. $(T, X) = (M_{11}, L_2(11))$: Let H be a Sylow 3-subgroup of T. Then $N_T(H) \cong M_9 : 2$ (see page 18 of the $\mathbb{ATLAS}$ of finite groups [12]) acts transitively on the cosets of X. Since $\mathrm{Aut}(M_{11}) = \mathrm{Inn}(M_{11})$, (i) and (ii) are satisfied.

3. $T = M_{12}$ and X is T-conjugate to one of the two copies of M_{11} in M_{12}; or $T = M_{24}$ and X is T-conjugate M_{23}: In each case, let H be a subgroup of T generated by a fixed point free element of order 3. When $T = M_{12}$, $N_T(H) \cong A_4 \times S_3$ (see [12, page 18]) is a maximal subgroup of T, and acts transitively on the cosets of X (for each copy of M_{11}). Also, the unique non-identity outer automorphism of M_{12} fixes the set of T-conjugates of H, so both (i) and (ii) are satisfied.

   When $T = M_{24}$, $N_T(H)$ has order 1008, and acts transitively on the cosets of X (using MAGMA [6], for example). Also, $\mathrm{Out}\,(T)$ is trivial. Thus, (i) and (ii) are again satisfied.

4. $T = L_2(p)$, with $p = 2^{f_1}3^{f_2} - 1 \geq 7$, $f_2 \leq 1$ and $X = C_p \rtimes C_{(p-1)/2}$. Then $|T : X| = p + 1 = 2^{f_1}3^{f_2}$. Assume first that $p \geq 7$, and let H be a dihedral group of order $p+1$ contained in T. Since T has a unique conjugacy class of maximal subgroups of dihedral groups of order $p+1$, (i) follows. Furthermore, $|T : H|$ and $|T : X|$ are coprime, so (ii) is also satisfied.

   This just leaves the case $p = 5$, but in this case $T = A_5$ and X is T-conjugate to D_{10} so taking $H = A_4$ gives us what we need.

□

Lemma 4.2.4. *Let $p \geq 7$ be a Mersenne prime, and let $L = T_1 \times T_2 \times \ldots \times T_e$, where each $T_i \cong L_2(p)$. Also, let A be a subgroup of L such that $|L : A| = 2^a 3$, for some a, and $|T_i : T_i \cap A| \in \{p+1, 3(p+1)\}$ for all i, with $|T_i : T_i \cap A| = 3(p+1)$ for at least one i. Then*

(i) $|L : A| = 3(p+1)^e$.

(ii) Let P be a Sylow p-subgroup of L. Then $N_L(P)$ is soluble, and has precisely 2^e orbits on the set Δ of (right) cosets of A in L, with $\binom{e}{k}$ orbits of size $3p^k$, for each k, $0 \leq k \leq e$.

Proof. We first prove Part (i) by induction on e, with the case $e = 1$ being trivial. So assume that $e > 1$, and fix k in the range $1 \leq k \leq e$ with $|T_k : T_k \cap A| = 3(p+1)$. Also, fix $i \neq k$, and set $\hat{T}_i := T_1 \times \ldots \times T_{i-1} \times T_{i+1} \times \ldots \times T_e$ and $\hat{A}_i = A \cap \hat{T}_i$. Then

$$|T_j : T_j \cap \hat{A}_i| = |T_j : T_j \cap \hat{T}_i \cap A| = |T_j : T_j \cap A| \in \{3(p+1), p+1\}$$

for each $j \neq i$. In particular, $|T_k : T_k \cap \hat{A}_i| = 3(p+1)$. Also, $|\hat{T}_i : \hat{A}_i| = |\hat{T}_i A : A|$ divides $|L : A|$, and is divisible by $|T_k : T_k \cap \hat{A}_i| = |T_k \hat{A}_i : \hat{A}_i| = 3(p+1)$, so $|\hat{T}_i : \hat{A}_i| = 2^{b_i}3$, for some $b_i \leq a$. Hence, the inductive hypothesis implies that $|\hat{T}_i : \hat{A}_i| = 3(p+1)^{e-1}$.

Assume that the claim in Part (i) does not hold. Then since $(p+1)^e$ is the highest power of 2 dividing $|L|$, we must have $|L : \hat{T}_i A| = |L : A|/|\hat{T}_i : \hat{A}_i| < p+1$. Hence, if $\rho_i : L \to T_i$ denotes projection onto T_i, then $|T_i : \rho_i(A)| = |\rho_i(L) : \rho_i(\hat{T}_i A)| = |L : \hat{T}_i A| < p+1$. But, as can be readily checked using [7, Tables 8.1 and 8.2], no maximal subgroup of $L_2(p)$ can have index a power of 2 and strictly less than $p+1$. Thus, we must have $\hat{T}_i A = L$, so A projects onto T_i. But then $A \cap T_i$ is a normal subgroup of T_i, so $A \cap T_i = 1$ or T_i. This contradicts $|T_i : A \cap T_i| \in \{p+1, 3(p+1)\}$, and Part (i) follows.

Finally, we prove (ii). Let $N := N_L(P)$. By Proposition 4.2.1 Part (iii), each $T_j \cap A$ is contained in a maximal subgroup $M_j := C_p \rtimes C_{(p-1)/2}$ of T_j, and $|T_j : T_j \cap A| \in \{p+1, 3(p+1)\}$. Thus, $T_j \cap A$ has a normal Sylow p-subgroup $P_j \cong C_p$. Let $\widetilde{P} := P_1 \times \ldots \times P_e$, so that $\widetilde{P}$ is a Sylow p-subgroup of L. Since P and $\widetilde{P}$ are conjugate in L, we may assume, for the purposes of proving Part (ii), that $\widetilde{P} = P$. Since $M_j = N_{T_j}(P_j)$ is soluble, $N = M_1 \times \ldots \times M_e$ is soluble. Also, $P \trianglelefteq A$ since P is a characteristic subgroup of $(T_1 \cap A) \times \ldots \times (T_e \cap A) \trianglelefteq A$, so $A \leq N$.

Suppose first that $e = 1$. Then $|L : A| = 3(p+1)$, so A has index 3 in N, since $|L : N| = |L : M_1| = p+1$. Let $x \in L \backslash N$, and let $\Gamma \subset \Delta$ be the N-orbit corresponding to Ax. Then $|\Gamma| = |N : N \cap A^x| = \frac{|L:N \cap A^x|}{|L:N|}$. Since $|L : N| = p+1$ is a power of 2 and $|L : N \cap A^x|$ is divisible by $|L : A^x| = 3(p+1)$, it follows that 3 divides $|\Gamma|$. Also, as mentioned above, A^x and N have unique Sylow p-subgroups P^x and P, respectively. Since x does not normalise P, we have $P^x \neq P$, so p, and hence $3p$, divides $|N : N \cap A^x| = |\Gamma|$. Since $|N : A| = 3$ and $|L : A| = 3(p+1)$, it

follows that $|\Gamma| = 3p$, which proves the claim in the case $e = 1$.

We now consider the general case. Fix $1 \leq i \leq e$, and $x_i \in T_i \backslash M_i$. Suppose first that $|T_i : T_i \cap A| = 3(p+1)$. From the previous paragraph, we see that M_i has precisely two orbits on the cosets of $T_i \cap A$ in T_i, of size 3 and $3p$, represented by A and Ax_i respectively. Next, assume that $|T_i : T_i \cap A| = p + 1$. Then $M_i = T_i \cap A$. Moreover, arguing as in the previous paragraph, p divides $|M_i : M_i \cap A^{x_i}|$, from which it follows that M_i again has two orbits on the cosets of $A \cap T_i$ in T_i, of size 1 and p, represented by A and Ax_i respectively.

Let $B := (T_1 \cap A) \times \ldots \times (T_e \cap A) \trianglelefteq A$. It is clear, from the previous paragraph, that $N = M_1 \times \ldots \times M_e$ has 2^e orbits on the cosets of B in L, represented by $Bt_1t_2 \ldots t_e$, where $t_i \in \{1, x_i\}$, for $1 \leq i \leq e$. Also, the orbit represented by the coset $Bt_1t_2 \ldots t_e$ has cardinality $3^d p^k$, where k is the number of subscripts i with $t_i \neq 1$, and d is the number of subscripts i with

$$|T_i : T_i \cap A| = 3(p+1). \tag{4.2.1}$$

Since $B \leq A$, N has at most 2^e orbits in Δ. Suppose there exist t_i, $\widetilde{t}_i \in \{1, x_i\}$ for $1 \leq i \leq e$, and $n = n_1n_2 \ldots n_e \in N$ (with $n_i \in M_i$), such that $At_1t_2 \ldots t_e = A(\widetilde{t}_1\widetilde{t}_2 \ldots \widetilde{t}_e)(n_1n_2 \ldots n_e)$. Then $t_i = a_i\widetilde{t}_i n_i$, where $a_1a_2 \ldots a_e \in A$. Since $A \leq N$, it follows that $t_i = 1$ if and only if $\widetilde{t}_i = 1$. Hence, $t_1t_2 \ldots t_e = \widetilde{t}_1\widetilde{t}_2 \ldots \widetilde{t}_e$. Thus, N has precisely 2^e orbits in Δ, represented by $At_1 \ldots t_e$, where $t_i \in \{1, x_i\}$. Since the size of the N-orbit corresponding to $At_1t_2 \ldots t_e$ is

$$|N : N \cap A^{t_1t_2\ldots t_e}| = \frac{|N : N \cap B^{t_1t_2\ldots t_e}|}{|N \cap A^{t_1t_2\ldots t_e} : N \cap B^{t_1t_2\ldots t_e}|} \geq \frac{|N : N \cap B^{t_1t_2\ldots t_e}|}{|A^{t_1t_2\ldots t_e} : B^{t_1t_2\ldots t_e}|},$$

and $|A^{t_1t_2\ldots t_e} : B^{t_1t_2\ldots t_e}| = |A : B| = |N : B|/|N : A| = 3^{d-1}$, it now follows from (4.2.1) that

$$|N : N \cap A^{t_1t_2\ldots t_e}| = \frac{|N : N \cap B^{t_1t_2\ldots t_e}|}{3^{d-1}} = 3p^k$$

where k is the number of subscripts i such that $t_i \neq 1$. This proves (ii). □

4.3 The proof of Theorem 1.2.4

First, we fix some notation which will be retained for the remainder of this section: Let G be a minimally transitive permutation group of degree $2^m 3$; let A be the stabiliser in G of a point δ; let L be a minimal normal subgroup of G; let Ω be the

set of L-orbits; let $K := \mathrm{Ker}(G^\Omega)$ be the kernel of the action of G on Ω; and finally, let Δ be the L-orbit containing δ.

Remark 4.3.1. G^Ω acts minimally transitively on Ω, by Lemma 3.2.1 Part (v). Note also that, if $|G : AL|$ is a power of 2, then G^Ω is a 2-group by Lemma 3.2.1 Part (vi).

We require the following easy proposition.

Proposition 4.3.2. *There exists a subgroup E of G such that $G = EL$ and $E \cap K$ is soluble.*

Proof. Consider the (set-wise) stabiliser $\mathrm{Stab}_G(\Delta)$ of Δ in G. Since L acts transitively on Δ, we have $LA = \mathrm{Stab}_G(\Delta)$. Let E be a subgroup of G minimal with the property that $EK = G$. Then $E \cap K$ is contained in the Frattini subgroup of E, and hence is soluble. Finally, $G = EK \leq E\,\mathrm{Stab}_G(\Delta) = ELA$, so $G = ELA$. Thus, $EL = G$ by minimal transitivity, as needed. □

Corollary 4.3.3. *If L is abelian, then the set of nonabelian chief factors of G equals the set of nonabelian chief factors of G^Ω. If L is nonabelian and $|\Omega| = |G : LA|$ is a power of 2, then L is the unique nonabelian chief factor of G.*

Proof. Let E be as in Proposition 4.3.2, and assume that either L is abelian or L is nonabelian and $|\Omega| = |G : LA|$ is a power of 2. For a finite group X write $\mathrm{NCF}(X)$ for the set of nonabelian chief factors of X. We need to prove that $\mathrm{NCF}(G) = \mathrm{NCF}(G^\Omega)$ if L is abelian, and $\mathrm{NCF}(G) = \{L\}$ otherwise. Note that if $|\Omega|$ is a power of 2 then G^Ω is soluble, by Remark 4.3.1.

Since E^Ω is transitive, the minimal transitivity of G^Ω implies that $G^\Omega = E^\Omega \cong E/E \cap K$. Since $E \cap K$ is soluble, it follows that $\mathrm{NCF}(G^\Omega) = \mathrm{NCF}(E)$. By hypothesis, either L is abelian, or L is nonabelian and E^Ω, and hence E, is soluble. Since $G = EL$, the claim follows, in either case. □

Proposition 4.3.4. *Suppose that $L = T_1 \times \ldots \times T_f$, where each T_i is isomorphic to a nonabelian simple group T. Without loss of generality, assume that $\mathrm{Ker}_L(\Delta) = T_{e+1} \times \ldots \times T_f$, so that $L^\Delta = T_1^\Delta \times \ldots \times T_e^\Delta$. Then*

(i) $T \cong L_2(p)$ for some Mersenne prime p,

(ii) $|T_i : T_i \cap A| \in \{p+1, 3(p+1)\}$ for each $1 \leq i \leq e$, and;

(iii) There exists at least one i in the range $1 \leq i \leq e$ such that $|T_i : T_i \cap A| = 3(p+1)$.

Proof. Suppose that the proposition is false, and set $X_i := T_i \cap A$. Note that $|T_i : X_i|$ divides $2^m 3$ for each i, by Lemma 3.2.1 Part (i). Hence, Proposition 4.2.1 implies that one of the following must hold:

(a) $T \ncong L_2(p)$, for any Mersenne prime p. Then by Proposition 4.2.1, either $T_i \cong M_{12}$ and each X_i is contained in one of the two conjugacy classes of M_{11} in M_{12}; or $(T_i, X_i) = (A_r, A_{r-1})$, $(A_6, L_2(5))$, $(M_{11}, L_2(11))$, (M_{24}, M_{23}), or $(L_2(p), C_p \rtimes C_{\frac{p-1}{2}})$ where p is a prime of the form $p = 2^{f_1}3 - 1$. Here, the group X_i is given up to conjugacy in T_i.

(b) $T \cong L_2(p)$ for some Mersenne prime p. In this case, Proposition 4.2.1 implies that $|T_i : X_i| = p + 1$ for all i. In particular, X_i is T_i-conjugate to the maximal subgroup $M_i := C_p \rtimes C_{\frac{p-1}{2}}$ of T_i. (We remark that it is here where we use the assumption that the proposition is false. Specifically, since $|T_i : X_i|$ divides $2^m 3$ for each i, Proposition 4.2.1 implies that X_i is T_i-conjugate to either M_i, or an index 3 subgroup of M_i. Hence $|T_i : X_i| \in \{p+1, 3(p+1)\}$ for each i. Thus, Part (iii) of the proposition must fail, forcing $|T_i : X_i|$ to be $p+1$, and hence for X_i to be T_i-conjugate to M_i, for each i.)

Fix $1 \leq i \leq e$, and write $T = T_i$. Note that T^Δ is isomorphic to T. Set $\Gamma := \delta^T \subset \Delta$, and set $X := T \cap A$. Then the pair (T, X) satisfies the hypothesis of Lemma 4.2.3. Thus, we conclude that T contains a proper subgroup H such that

(i) H and H^α are conjugate in T for each automorphism $\alpha \in \mathrm{Aut}(T)$; and

(ii) $N_T(H)^\Gamma$ is transitive.

Fix a T-orbit Γ' in Δ. We claim that $N_T(H)^{\Gamma'}$ is transitive. By Lemma 3.2.1 Part (ii), $T^{\Gamma'}$ is permutation isomorphic to T^Γ. Hence, by (ii) above, there exists an automorphism α of T such that $N_T(H)^\alpha = N_T(H^\alpha)$ acts transitively on Γ'. Since H is T-conjugate to H^α, it follows that $N_T(H)$ is T-conjugate to $N_T(H)^\alpha$. Thus, $N_T(H)$ acts transitively on Γ', as claimed.

Since $T_i \cong T_j$ for all i, j, we can choose the subgroup $H_j < T_j$ corresponding to H, and the subgroup $N_j < T_j$ corresponding to $N_T(H)$, for each $1 \leq j \leq f$. Furthermore, each group X_i is determined up to conjugacy in T_i by (a) and (b) above. Hence, by the previous paragraph

$$N_j \text{ acts transitively on each } T_j\text{-orbit in } \Delta \text{ whenever } 1 \leq j \leq e. \tag{4.3.1}$$

Set $\widetilde{H} = H_1 \times H_2 \times \ldots \times H_f < L$, and $N := N_1 \times N_2 \times \ldots \times N_f$. Now, note that $N \leq N_L(\widetilde{H})$. Thus, $N_1^\Delta \times N_2^\Delta \times \ldots \times N_e^\Delta = N^\Delta \leq N_L(\widetilde{H})^\Delta$.

We will now prove that N^Δ is transitive. Indeed, let $\epsilon \in \Delta$, and let $x \in L$ such that $\delta^x = \epsilon$. Write $x = t_1 t_2 \ldots t_e$, with $t_j \in T_j$. By (ii) above, N_1 acts transitively on δ^{T_1}. Hence, there exists $n_1 \in N_1$ such that $\delta^{t_1} = \delta^{n_1}$. We now inductively define the permutations n_2, ..., n_e by choosing $n_j \in N_j$ such that $(\delta^{n_1 \cdots n_{j-1}})^{n_j} = \delta^{n_1 \cdots n_{j-1} t_j}$ (this is possible since N_j acts transitively on $(\delta^{n_1 \cdots n_{j-1}})^{T_j}$, by (4.3.1)). Then

$$\begin{aligned}\epsilon = \delta^{t_1 t_2 \cdots t_e} = (\delta^{t_1})^{t_2 \cdots t_e} = \delta^{n_1 t_2 \cdots t_e} = (\delta^{n_1 t_2})^{t_3 \cdots t_e} \\ = \delta^{n_1 n_2 t_3 \cdots t_e} = (\delta^{n_1 n_2 t_3})^{t_4 \cdots t_e} = \cdots = \delta^{n_1 n_2 \cdots n_e}\end{aligned}$$

Thus

$$N^\Delta \text{ is transitive, as claimed.} \tag{4.3.2}$$

Finally, let $\alpha \in \mathrm{Aut}\,(L) \cong \mathrm{Aut}\,(T) \wr \mathrm{Sym}(f)$. Then there exists $\tau \in \mathrm{Sym}\,(f)$ and $\alpha_i \in \mathrm{Aut}\,(T)$ such that

$$\begin{aligned}\widetilde{H}^\alpha &= H_{1^\tau}^{\alpha_1} \times H_{2^\tau}^{\alpha_2} \times \ldots \times H_{f^\tau}^{\alpha_f} \\ &= H_1^{\alpha_{1^{\tau^{-1}}}} \times H_2^{\alpha_{2^{\tau^{-1}}}} \times \ldots \times H_f^{\alpha_{f^{\tau^{-1}}}}\end{aligned}$$

By (i) above, there exists, for each $1 \leq i \leq f$, an element $t_i \in T_i$ such that $H_i^{\alpha_{i^{\tau^{-1}}}} = H_i^{t_i}$. Hence

$$\widetilde{H}^\alpha = H_1^{t_1} \times H_2^{t_2} \times \ldots \times H_f^{t_f} = \widetilde{H}^{t_1 t_2 \ldots t_f}.$$

Thus, $\widetilde{H}$ and $\widetilde{H}^\alpha$ are conjugate in L for all $\alpha \in \mathrm{Aut}\,(L)$. Lemma 4.2.2 then implies that $G = N_G(\widetilde{H})L$. Thus, $N_G(\widetilde{H})$ acts transitively on the set Ω of L-orbits. But $N_G(\widetilde{H})$ also acts transitively on the fixed L-orbit Δ, by (4.3.2). Hence, $N_G(\widetilde{H})$ is a transitive subgroup of G. By minimal transitivity of G, it follows that $N_G(\widetilde{H}) = G$, so $\widetilde{H}$ is normal in G. But this is a contradiction, since $1 < \widetilde{H} < L$ and L is a minimal normal subgroup of G. The proof is complete. □

Property (iii) of Proposition 4.3.4 immediately implies the following.

Corollary 4.3.5. *Suppose that L is isomorphic to a direct product of copies of $L_2(p)$, where p is a Mersenne prime. Then $|\Delta|$ is divisible by 3.*

Finally, we are ready to prove Theorem 1.2.4.

Proof of Theorem 1.2.4. Assume that G is a counterexample to the theorem of minimal degree. Note that $|\Omega| = |G : LA|$ divides $|G : A| = 2^m 3$, and is less than $2^m 3$. Furthermore, a minimally transitive group of 2-power degree is soluble by Remark 4.3.1. Hence, the minimality of G as a counterexample implies that $G^\Omega = G/K$ satisfies either (i) or (ii) in the statement of the theorem.

If L is abelian, then Corollary 4.3.3 implies that the set of nonabelian chief factors of G equals the set of nonabelian chief factors of G^Ω. Thus, the result follow from the inductive hypothesis in this case. So we may assume that $L = T_1 \times T_2 \times \ldots \times T_f$, where each T_i is isomorphic to a nonabelian finite simple group T. Furthermore, Proposition 4.3.4 then implies that $T \cong L_2(p)$, where p is a Mersenne prime. Also, 3 divides $|\Delta|$ by Corollary 4.3.5. But then $|\Omega| = |G : LA|$ is a power of 2, so L is the unique nonabelian chief factor of G by Corollary 4.3.3. This contradiction completes the proof. □

We also deduce two corollaries which will be vital in our application of Theorem 5.4.15 (see Chapter 5).

Corollary 4.3.6. *Assume that G is insoluble, and let $p := 2^a - 1$ be a Mersenne prime such that G has a unique nonabelian chief factor isomorphic to a direct product of f copies of $L_2(p)$. Then there exists a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that*

(i) $m = ea + t$, and;

(ii) For some soluble subgroup N of G, N has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p^k \times 2^{t-t_1}$, for each k, $0 \leq k \leq e$.

Proof. Let E be as in Proposition 4.3.2, so that $G = EL$, and $E \cap K$ is soluble. We prove the claim by induction on m. Suppose first that L is abelian. Then since $EL = G$ and $E \cap K$ is soluble, $G^\Omega = E^\Omega$ is insoluble. Hence $|\Omega| = 2^{\widetilde{m}}3$ and $|\Delta| = 2^{m-\widetilde{m}}$, for some $\widetilde{m}$ with $1 \leq \widetilde{m} < m$, by Lemma 3.2.1 Parts (i) and (vi). The inductive hypothesis then implies that there exists a triple $(\widetilde{e}, \widetilde{t_1}, \widetilde{t})$ such that

1. $\widetilde{m} = \widetilde{e}a + \widetilde{t}$, and;
2. For some soluble subgroup $\widetilde{N}$ of E^Ω, $\widetilde{N}$ has $2^{\widetilde{e}+\widetilde{t_1}}$ orbits, with $\binom{\widetilde{e}}{k}2^{\widetilde{t_1}}$ of them of length $3p^k \times 2^{\widetilde{t}-\widetilde{t_1}}$, for each k, $0 \leq k \leq \widetilde{e}$.

Set $e := \widetilde{e}$, $t := m - \widetilde{m} + \widetilde{t}$, and $t_1 := \widetilde{t_1}$, so that $m = ea + t$, which is what we need for (i). Also, let $Y \leq E$ such that $Y^\Omega = \widetilde{N}$, and set $N := LY$. Then N is soluble, since the groups Y^Ω, $Y \cap K$ and L are soluble. Moreover, N acts transitively on each L-orbit, since $L \leq N$. Since each L-orbit has size $2^{m-\widetilde{m}}$, it follows that N has 2^{e+t_1} orbits, with $\binom{e}{k} \times 2^{t_1}$ of them of length $3p^k 2^{\widetilde{t}-\widetilde{t_1}+m-\widetilde{m}} = 3p^k 2^{t-t_1}$. This gives us what we need.

So assume that $L = T_1 \times T_2 \times \ldots \times T_f$, where each $T_i \cong L_2(p)$. By Proposition 4.2.1 Part (iii), $T_i \cap A$ is contained in the maximal subgroup $M_i \cong C_p \rtimes C_{(p-1)/2}$ of T_i, and $|T_i : T_i \cap A| \in \{p+1, 3(p+1)\}$ for all i. Furthermore, Proposition 4.3.4 implies that there exists at least one subscript i such that $|T_i : T_i \cap A| = 3(p+1)$. Lemma 4.2.4 now implies that $|\Delta| = |L : L \cap A| = 3(p+1)^e = 2^{ea}3$, where e is the number of direct factors of L acting non-trivially on Δ. It also follows that $|\Omega| = 2^{m-ea}$.

By relabeling the T_i if necessary, we may write $L^\Delta = T_1^\Delta \times T_2^\Delta \times \ldots \times T_e^\Delta$. Let P be a Sylow p-subgroup of L, and let $N := N_L(P)$. By Lemma 4.2.4 Part (ii), N is soluble, and $N_L(P)^\Delta = N_{L^\Delta}(P^\Delta)$ has 2^e orbits on Δ, with $\binom{e}{k}$ of size $3p^k$, for each $0 \leq k \leq e$. Since the action of L on each L-orbit is permutation isomorphic to the action of L on Δ, it follows that $N := N_L(P)$ has 2^e orbits on each L-orbit, with $\binom{e}{k}$ of size $3p^k$, for each $0 \leq k \leq e$. Also, N acts trivially on the set Ω of L-orbits, so N has 2^{e+m-ea} orbits in total, with $2^{m-ea}\binom{e}{k}$ of them of size $3p^k$, for each $0 \leq k \leq e$. Setting $t := m - ea$ and $t_1 := t$ now gives us what we need, and completes the proof. □

Corollary 4.3.7. *Let S be a transitive permutation group of degree $s := 2^m 3$, and assume that S contains no soluble transitive subgroups. Then there exists a Mersenne prime $p := 2^a - 1$ and a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that*

(i) $m = ea + t$, and;

(ii) For some soluble subgroup N of S, N has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p^k \times 2^{t-t_1}$, for each k, $0 \leq k \leq e$.

Proof. Let G be a minimally transitive subgroup of S. Then G is insoluble, so Corollary 4.3.6 applies, and the result follows. □

Chapter 5

Generating submodules of induced modules for finite groups

5.1 Introduction

The purpose of this thesis is to derive upper bounds on minimal generator numbers in certain classes of permutation groups. As can be seen from Section 2.1.2, this essentially amounts to deriving upper bounds on $d(G)$ for subgroups G of wreath products $R \wr S$. Our main strategy for doing this will be to reduce modulo the base group B of $R \wr S$ and use induction to bound $d(G/G \cap B)$. In this way, all that remains is to investigate the contribution of $G \cap B$ to $d(G)$: The purpose of this chapter is to carry out such an investigation.

As we will show in Lemma 6.2.5, the group $G \cap B$ is built, as a normal subgroup of G, from submodules of induced modules for G, and nonabelian chief factors of G. Thus, the main aim of the chapter will be to derive upper bounds for generator numbers in submodules of induced modules. The strategy to do this will be to first view soluble groups as certain partially ordered sets: We prove some properties of these partially ordered sets in Section 5.2. Our main results are Theorem 5.4.4 and Theorem 5.4.15, which are proved in Sections 5.4.1 and 5.4.2 respectively. We remark that Theorem 5.4.4 improves [8, Theorem 1.5], while Theorem 5.4.15 improves [37, Lemma 4].

5.2 Partially ordered sets

Let $P = (P, \preccurlyeq)$ be a finite partially ordered set, and let $w(P)$ denote the *width* of P. That is, $w(P)$ is the maximum cardinality of an antichain in P. Suppose now that, with respect to $\preccurlyeq$, P is a cartesian product of chains, and write $P = P_1 \times P_2 \times \ldots \times P_t$, where each P_i is a chain of cardinality k_i. Then P is poset-isomorphic to the set of divisors of the positive integer $m = p_1^{k_1-1} p_2^{k_2-1} \ldots p_t^{k_t-1}$, where p_1, p_2, ..., p_t are distinct primes. We make this identification without further comment.

Next, recall that each divisor d of m can be written uniquely in the form $d = p_1^{r_1} p_2^{r_2} \ldots p_t^{r_t}$, where $0 \le r_i \le k_i - 1$, for each i, $1 \le i \le t$. In this case, the *rank* of d is defined as $r(d) = \sum_{i=1}^{t} r_i$. For $0 \le k \le K := \sum_{i=1}^{t}(k_i - 1)$, let R_k denote the set of elements of P of rank k; clearly R_k is an antichain in P. In fact, it is proved in [16] that $w(P) = \max |R_k|$. This maximal rank set occurs at $k = \lfloor K/2 \rfloor$, and hence, by [2, Theorem 2], we have

$$w(P) \le \left\lfloor \frac{s}{2^K} \binom{K}{\lfloor K/2 \rfloor} \right\rfloor$$

where $s := |P| = \prod_{i=1}^{t} k_i$ (note that equality holds when t is even and each k_i is 2, so this upper bound is best possible). Stated more concisely, we have

Lemma 5.2.1. *Suppose that a partially ordered set P, of cardinality $s \ge 2$, is a cartesian product of the chains P_1, P_2, ..., P_t, where each P_i has cardinality k_i. Then*

$$w(P) \le \left\lfloor \frac{s}{2^K} \binom{K}{\lfloor K/2 \rfloor} \right\rfloor,$$

where $K := \sum_{i=1}^{t}(k_i - 1)$.

We now define a constant b,

$$b := \sqrt{\frac{2}{\pi}}.$$

Proposition 5.2.2. *Let K be a positive integer. Then*

$$\binom{K}{\lfloor K/2 \rfloor} \le \frac{b 2^K}{\sqrt{K}}. \tag{5.2.1}$$

Proof. [1] First consider the case where $K = 2t$ ($t \in \mathbb{N}$), and note that

$$2t\left[\binom{2t}{t}\frac{1}{4^t}\right]^2 = \frac{1}{2}\left(\frac{3}{2}\frac{3}{4}\right)\left(\frac{5}{4}\frac{5}{6}\right)\cdots\left(\frac{2t-1}{2t-2}\frac{2t-1}{2t}\right) = \frac{1}{2}\prod_{j=2}^{t}\left(1+\frac{1}{4j(j-1)}\right)$$

By Wallis' Formula, the expression in the middle converges to $2/\pi$. Hence, since the expression on the right is increasing, we have $2t\left[\binom{2t}{t}\frac{1}{4^t}\right]^2 \leq 2/\pi$, that is, $\binom{2t}{t} \leq b4^t/\sqrt{2t}$, as claimed. If K is odd, we have $\binom{K}{\lfloor K/2\rfloor} = \frac{1}{2}\binom{K+1}{\lfloor (K+1)/2\rfloor}$, and the bound in (5.2.2) follows from the even case above. □

Corollary 5.2.3. *Suppose that a partially ordered set P, of cardinality $s \geq 2$, is a cartesian product of t chains. Let k_i and K be as in Lemma 5.2.1. Then*

$$w(P) \leq \left\lfloor \frac{s}{2^K}\binom{K}{\lfloor K/2\rfloor}\right\rfloor \leq \left\lfloor \frac{bs}{\sqrt{K}}\right\rfloor \leq \left\lfloor \frac{bs}{\sqrt{\log s}}\right\rfloor.$$

Furthermore, if each chain has the same cardinality p, then $w(P) \leq \lfloor bp^t/\sqrt{t(p-1)}\rfloor$.

Proof. By Lemma 5.2.1 and Proposition 5.2.2, we have

$$w(P) \leq \frac{s}{2^K}\binom{K}{\lfloor K/2\rfloor} \leq \frac{s}{2^K}\left(\frac{b2^K}{\sqrt{K}}\right) = \frac{bs}{\sqrt{K}}$$

If each $k_i = p$, then $K = t(p-1)$, and the second part of the claim follows. Since $K = \sum_{i=1}^{t}(k_i - 1) \geq \sum_{i=1}^{t}\log k_i = \log s$, the first part also follows, and the proof is complete. □

5.3 Preliminary results on induced modules for finite groups

5.3.1 Composition factors in induced modules

Let $\mathbb{F}$ be a field, let G be a finite group, and let V be a module for G over $\mathbb{F}$. Let

$$0 = N_0 < N_1 < \ldots < N_a = V$$

be a G-composition series for V, and say that a factor N_i/N_{i-1} is *complemented* if there exists a submodule S_i of V containing N_{i-1} such that $V/N_{i-1} = N_i/N_{i-1} \oplus$

[1] The idea for this bound arose from a discussion at the url http://math.stackexchange.com/questions/58560/elementary-central-binomial-coefficient-estimates.

S_i/N_{i-1}. Also, for an irreducible $\mathbb{F}[G]$-module W, write $t_W(V)$ for the number of complemented composition factors of V isomorphic to W.

Now, fix an irreducible $\mathbb{F}[G]$-module W with $t_W(V) \geq 1$. Then there exists a submodule M of V with the property that V/M is G-isomorphic to W: Define $R_W(V)$ to be the intersection of all such M. In particular, $R_W(V)$ contains the radical $\mathrm{Rad}(V)$ of V.

Lemma 5.3.1. $V/R_W(V) \cong W^{\oplus t_W(V)}$.

Proof. Let $t := t_W(V)$, and write $R := R_W(V) = M_1 \cap M_2 \cap \ldots \cap M_e$, where V/M_i is isomorphic to W. Then

$$V/R \leq (V/M_1) \oplus (V/M_2) \oplus \ldots \oplus (V/M_e)$$

and hence V/R is a direct sum of k copies of W, where $k \leq e$. Since $t_W(V) = t_W(V/R)$, we have $t = k$, and this completes the proof. □

Lemma 5.3.2. *Suppose that $V = U\uparrow_H^G$, for a subgroup H of G and an H-module U, and suppose that W is a 1-dimensional $\mathbb{F}[G]$-module. Then $t_W(V) \leq \dim U$.*

Proof. Let $R = R_W(V)$ and $t = t_W(V)$. Writing bars to denote reduction modulo R, we have

$$\overline{V} = \overline{N_1} \oplus \overline{N_2} \oplus \ldots \oplus \overline{N_t}$$

where each $\overline{N_i}$ is isomorphic to W. In particular, if we write

$$V/\mathrm{Rad}(V) = \sum_{X \text{ an irreducible } \mathbb{F}[G]\text{-module}} X^{f_X(V)},$$

then we have $t \leq f_W(V)$. Moreover, since $\dim W = 1$, we have

$$f_W(V) = \dim \mathrm{Hom}_{\mathbb{F}[G]}(V, W) = \dim \mathrm{Hom}_{\mathbb{F}[H]}(U, W\downarrow_H) = f_{W\downarrow_H}(U) \leq \dim U$$

where the second equality above follows from Theorem 2.2.5. This completes the proof. □

We will need an easy consequence of Lemma 5.3.2. To state it, we first require two definitions and a remark.

Definition 5.3.3. Let G be a non-trivial finite group, and $\mathbb{F}$ a field. A *projective representation* of G of dimension m over $\mathbb{F}$ is a homomorphism $\rho : G \to PGL_m(\mathbb{F})$.

Define

$R_{\mathbb{F}}(G) := \min\{m : G \text{ has a non-trivial representation of dimension } m \text{ over } \mathbb{F}\}$; and
$\overline{R}_{\mathbb{F}}(G) := \min\{m : G \text{ has a non-trivial projective representation of dimension } m \text{ over } \mathbb{F}\}$.

Also define

$$\overline{R}(G) := \min\left\{\overline{R}_{\mathbb{F}}(G) : \mathbb{F} \text{ a field}\right\}$$

Definition 5.3.4. Let G be a finite group, let $\mathbb{F}$ be a field, and let V be an $\mathbb{F}[G]$-module. Define $d_G(V)$ to be the minimal number of elements required to generate V as an $\mathbb{F}[G]$-module.

Remark 5.3.5. Let G, $\mathbb{F}$ and V be as in Definition 5.3.4, and let t be the number of complemented G-composition factors of V. We claim that $d_G(V) \leq t$. Note first that t is precisely the number of irreducible constituents of $V/\operatorname{Rad}(V)$. In particular, it follows that $d_G(V/\operatorname{Rad}(V)) \leq t$: let $v_1, \ldots, v_t \in V$ such that $V/\operatorname{Rad}(V)$ is generated, as a G-module, by $\{\operatorname{Rad}(V)+v_1, \ldots, \operatorname{Rad}(V)+v_t\}$. Let M be the G-submodule of V generated by $\{v_1, \ldots, v_t\}$. Then $V = M + \operatorname{Rad}(V)$. Since $\operatorname{Rad}(V)$ is contained in every maximal submodule of V, it follows that $V = M$, and hence $d_G(V) \leq t$, as claimed.

The corollary of Lemma 5.3.2 can now be stated as follows.

Corollary 5.3.6. *Let G be a finite group, let H be a subgroup of G, and let U be an H-module, over a field $\mathbb{F}$. Let $V := U\uparrow_H^G$. Then*

$$d_G(V) \leq \frac{\dim U|G:H| - \dim U}{R_{\mathbb{F}}(G)} + \dim U.$$

Proof. Write t for the number of complemented G-composition factors of V which are not isomorphic to the trivial G-module 1_G. By Remark 5.3.5, we have

$$d_G(V) \leq t_{1_G}(V) + t.$$

Since $\dim V = \dim U|G:H|$, we have

$$t \leq \frac{\dim U|G:H| - \dim U}{R_{\mathbb{F}}(G)}.$$

The result now follows immediately from Lemma 5.3.2. □

5.3.2 Induced modules for Frattini extensions of nonabelian simple groups

In this subsection, we make some observations on modules for Frattini extensions of nonabelian simple groups. That is, modules for groups G with $G/\Phi(G)$ a non-abelian simple group. For the terminology used in the proof, we refer the reader to Section 2.3.

The main result of this section reads as follows.

Proposition 5.3.7. *Let G be a finite group with a normal subgroup $N \leq \Phi(G)$ such that $G/N \cong T$, where T is a non-abelian finite simple group. Also, let W be a nontrivial irreducible G-module, over an arbitrary field $\mathbb{F}$. Then*

(i) Each proper normal subgroup of G is contained in N. In particular, $N = \Phi(G)$.

(ii) $\mathrm{Ker}_G(W)$*, the kernel of the action of G on W, is contained in N.*

(iii) $n := \dim W \geq \overline{R}(T)$.

Proof. Part (i) follows since $N \leq \Phi(G)$ and G/N is simple. Part (ii) now follows from Part (i) since W is non-trivial.

We will now prove (iii). In what follows, we will use the terminology and theory discussed in Section 2.3. By (ii), we may assume that G is faithful on W. In particular, we may view G as a subgroup of $GL_n(\mathbb{F})$. Let L be a normal subgroup of G, and assume that $W\downarrow_L$ is non-homogeneous. If K is the kernel of the action of G on the homogeneous components of $W\downarrow_L$, then K is a proper normal subgroup of G, so $K \leq N$ by Part (i). Thus, $HN < G$ for some stabiliser H of a homogeneous component. Hence, $|G : H| \geq |G : HN| = |G/N : HN/N| \geq \overline{R}_{\mathbb{F}}(T)$, since any proper subgroup E of T gives rise to a nontrivial permutation representation for T of dimension $|T : E|$ over $\mathbb{F}$ (a non-trivial projective representation of dimension $|T : E|$ is then achieved by reducing modulo scalars). Thus, the number of homogeneous components is at least $\overline{R}_{\mathbb{F}}(T)$, and the result follows.

So we may assume that $W\downarrow_L$ is homogeneous for each normal subgroup L of G. Hence, by Lemma 2.3.6, we may assume that $Z(G)$ is cyclic and that each abelian characteristic subgroup of G is contained in $Z(GL_n(\mathbb{F}))$.

Let L be the generalised Fitting subgroup of G, and extend the field $\mathbb{F}$ so that $\mathbb{F}$ is a splitting field for each subgroup of L, and so that the resulting field extension is normal (see Remark 2.3.8).

We distinguish two cases.

1. L is soluble. In this case, since $L > Z(G)$, $O_r(G)$ must be non-central, for some prime r, and $O_r(G)C_G(O_r(G)) \geq L$. Also, since $O_r(G)$ is non-central, we have $O_r(G)$, $C_G(O_r(G)) \leq N$ by Part (i). Thus, since $N \leq \Phi(G) \leq L$, it follows that $N = L = O_r(G)C_G(O_r(G))$. Hence, by [35, Lemma 1.7], there exists a positive integer m such that

   (1) $O_r(G)$ is a central product of its intersection with $Z := Z(G)$ and an extraspecial group E of order r^{1+2m};

   (2) $Z(E)$ coincides with the subgroup of Z of order r (recall that Z is cyclic);

   (3) EZ/Z is a completely reducible $\mathbb{F}_r[G]$-module under conjugation; and

   (4) $C_{G/Z}(EZ/Z) = O_r(G)C_G(O_r(G))/Z$.

   It follows from (4) that $T \cong G/N = G/O_r(G)C_G(O_r(G))$ is a non-trivial completely reducible subgroup of $GL_{2m}(r)$. It then follows that

   $$\overline{R}_{\mathbb{F}_r}(T) \leq 2m. \tag{5.3.1}$$

   Next, by Lemma 2.3.7, $W\downarrow_E$ is completely reducible and its irreducible constituents are non-trivial. Let U be such a constituent. Since $\mathbb{F}$ is a splitting field for E, U is absolutely irreducible. Hence, $\dim U \geq r^m$, by [24, Theorem 5.5]. Thus, by (5.3.1), we have

   $$\overline{R}(T) \leq \overline{R}_{\mathbb{F}_r}(T) \leq 2m \leq r^m \leq \dim U \leq \dim W,$$

   which gives us what we need.

2. L is insoluble. By [25, Lemma 2.14], L contains a normal subgroup X of G of the form $X = S_1 \circ \ldots \circ S_t$, where each S_i is isomorphic to a quasisimple group S. But since $N \leq \Phi(G)$, N is nilpotent. Also, G/N is simple, so we must have $G = X$ and G is quasisimple. In particular, $N = Z \leq Z(GL_n(\mathbb{F}))$. Hence, $T \cong G/Z \leq PGL_n(\mathbb{F})$ and $\dim W \geq \overline{R}_{\mathbb{F}}(T) \geq \overline{R}(T)$, as required.

This completes the proof. □

We close this section with an easy lemma concerning the alternating group $\mathrm{Alt}(d)$.

Lemma 5.3.8. *Let $D \cong \mathrm{Alt}(d)$ be the alternating group of degree $d \geq 5$, and let p be prime. Then D contains a soluble subgroup E with at most two orbits on $\{1, \ldots, d\}$, such that each orbit has p'-length.*

Proof. Assume first that $p = 2$. Then since d is either odd, or a sum of two odd numbers, we can take $E := \langle x_1 x_2 \rangle$, where x_1 is a cycle of odd length, either $x_2 = 1$ or x_2 is a cycle of odd length, and d is the sum of the orders (i.e. lengths) of x_1 and x_2.

So assume that $p > 2$, and write $d = tp + k$, where $0 \leq k \leq p - 1$. If $k \neq p - 1$, then take E_1 to be a soluble transitive subgroup of $\mathrm{Alt}(tp - 1)$, and take E_2 to be a soluble transitive subgroup of $\mathrm{Alt}(k + 1)$. If $k = p - 1$, then take E_1 to be a soluble transitive subgroup of $\mathrm{Alt}(tp + 1)$, and take E_2 to be a soluble transitive subgroup of $\mathrm{Alt}(k - 1)$ (note that $k - 1 > 0$ since $p > 2$). Finally, taking $E := E_1 \times E_2 \leq D$ give us what we need, and proves the claim. □

5.4 Induced modules for finite groups

We begin with some terminology.

Definition 5.4.1. Let M be a group, acted on by another group G. A *G-subgroup* of M is a subgroup of M which is stabilised by G. We say that M is *generated as a G-group* by $X \subset M$, and write $M = \langle X \rangle_G$, if no proper G-subgroup of M contains X. We will write $d_G(M)$ for the cardinality of the smallest subset X of M satisfying $\langle X \rangle_G = M$. Finally, write $M^* := M \backslash \{1\}$.

Note that the definition of $d_G(M)$ is consistent with the notation introduced in Definition 5.3.4 in the case where M is a G-module.

Definition 5.4.2. Let G be a group, acting on a set Ω. Write $\chi(G, \Omega)$ for the number of orbits of G on Ω.

The purpose of this section is to derive upper bounds for $d_G(M)$ when M is a submodule of an induced module for G. To this end, we introduce some notation which will be retained for the remainder of the section:

- Let G be a finite group.
- Fix a subgroup H of G of index $s \geq 2$.
- Fix a subgroup H_1 of H of index $d \geq 1$.

- Let U be a module for H_1 of dimension a, over a field $\mathbb{F}$.
- Let $K := \mathrm{core}_G(H)$, and fix a subgroup K' of K.
- Set $V := U \uparrow_{H_1}^{H}$ and $W := V \uparrow_{H}^{G}$ to be the induced modules. Note also that $V \uparrow_{H}^{G} \cong U \uparrow_{H_1}^{G}$.
- Denote the set of right cosets of H in G [respectively H_1 in H] by Ω [resp. Ω_1].
- Define

$$m := m(K') = \min\{\chi(Q^{\Omega_1}, \Omega_1) : Q \leq K' \text{ and } Q^V \text{ is semisimple}\}.$$

We do not exclude the case $d = 1$, that is, $H = H_1$.

5.4.1 Induced modules: The soluble case

This section is essentially an analogue of [8, Section 5]. We first recall the constant b,

$$b := \sqrt{\frac{2}{\pi}}.$$

We will also recall, from Chapter 1, the following definition.

Definition 5.4.3. For a positive integer s with prime factorisation $s = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, set $\omega(s) := \sum r_i$, $\omega_1(s) := \sum r_i p_i$, $K(s) := \omega_1(s) - \omega(s) = \sum r_i(p_i - 1)$ and

$$\widetilde{\omega}(s) = \frac{s}{2^{K(s)}} \binom{K(s)}{\left\lfloor \frac{K(s)}{2} \right\rfloor}.$$

The main result of this section reads as follows.

Theorem 5.4.4. *Suppose that G^Ω contains a soluble transitive subgroup, and let M be a submodule of W. Also, denote by $\chi = \chi(K, V^*)$ the number of orbits of K on the non-zero elements of V. Then*

$$d_G(M) \leq \min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi\right\} \widetilde{\omega}(s) \leq \min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi\right\} \left\lfloor \frac{bs}{\sqrt{\log s}} \right\rfloor$$

where $b := \sqrt{2/\pi}$. *Furthermore, if* $s = p^t$, *with* p *prime, then*

$$d_G(M) \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\}\left\lfloor \frac{bp^t}{\sqrt{t(p-1)}}\right\rfloor.$$

Remark 5.4.5. If K has infinitely many orbits on the non-zero elements of V, then we assume, in Theorem 5.4.4, and whenever it is used in the remainder of the thesis, that

$$\min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\} = \frac{ad-am}{R_{\mathbb{F}}(K')} + am.$$

We begin our work towards the proof of Theorem 5.4.4 by first collecting a series of lemmas from [8, Section 5].

Lemma 5.4.6 ([8], Lemma 5.1). *Suppose that* G^Ω *contains a soluble transitive subgroup. Then there is a right transversal* $\mathcal{T}$ *to* H *in* G, *with a partial order* $\preccurlyeq$ *and a full order* $\leqslant$, *satisfying the following properties:*

(i) Whenever t_1, t_2, $t_3 \in \mathcal{T}$ *with* $t_1 < t_2 \preccurlyeq t_3$, *we have* $t_4 < t_3$, *where* t_4 *is the unique element of* $\mathcal{T}$ *such that* $t_1 t_2^{-1} t_3 \in Ht_4$.

(ii) With respect to this partial order, $\mathcal{T}$ *is a cartesian product of* k *chains, of length* p_1, p_2, …, p_k, *where* $k = \omega(s)$, *and* p_1, p_2, …, p_k *denote the (not necessarily distinct) prime divisors of* s.

Proof. Let F be a subgroup of G such that F^Ω is soluble and transitive. By [8, Lemma 5.1], there exists a right transversal $\mathcal{T}$ for $F \cap H$ in F such that the image $\mathcal{T}^\Omega$ has a partial order $\preccurlyeq'$ and a full order $\leqslant'$ satisfying

(a) Whenever t_1, t_2, $t_3 \in \mathcal{T}$ with ${t_1}^\Omega <' {t_2}^\Omega \preccurlyeq' {t_3}^\Omega$, we have ${t_4}^\Omega <' {t_3}^\Omega$, where t_4 is the unique element of $\mathcal{T}$ such that $(t_1 t_2^{-1} t_3)^\Omega \in (F \cap H)^\Omega {t_4}^\Omega$.

(b) With respect to this partial order, $\mathcal{T}^\Omega$ is a cartesian product of k chains, of length p_1, p_2, …, p_k, where $k = \omega(|F : F \cap H|) = \omega(|G : H|) = \omega(s)$, and p_1, p_2, …, p_k denote the (not necessarily distinct) prime divisors of s.

For t_1, $t_2 \in \mathcal{T}$, say now that $t_1 \preccurlyeq t_2$ if ${t_1}^\Omega \preccurlyeq' {t_2}^\Omega$, and $t_1 \leqslant t_2$ if ${t_1}^\Omega \leqslant' {t_2}^\Omega$. Since F^Ω acts transitively on the set of cosets of H in G, $\mathcal{T}$ is a right transversal for H in G. By definition, (a) and (b) above imply that (i) and (ii) hold for this choice of $\preccurlyeq$ and $\leqslant$. This gives us what we need. □

For the remainder of Section 5.4 assume that G^Ω contains a soluble transitive subgroup, and fix $\mathcal{T}$ to be a right transversal for H in G as exhibited in Lemma 5.4.6. Then we may write the induced module $W = V \uparrow_H^G$ as $W = \bigoplus_{t\in\mathcal{T}} V \otimes t$, where the action of G is given by

$$(v \otimes t)^{ht'} = v^{h_1} \otimes t_1,$$

where $tht' = h_1 t_1$, h, $h_1 \in H$, t, t', $t_1 \in \mathcal{T}$. Thus, each element w in W may be written as $w = \sum_{t\in\mathcal{T}} v(w,t) \otimes t$, with uniquely determined coefficients $v(w,t)$ in V (see Definition 2.2.2).

Definition 5.4.7 ([8], Section 5). Let $w \in W$ be non-zero. The *height* of w, written $\tau(w)$, is the largest element of the set $\{t \in \mathcal{T} : v(w,t) \neq 0\}$, with respect to the full order $\leqslant$. Also, we define $\mu(w) := v(w, \tau(w))$. Thus, $\mu(w)$ is non-zero, and $v(w,t) = 0$ whenever $t > \tau(w)$. The element $\mu(w) \otimes \tau(w)$ is called the *leading summand* of w.

Remark 5.4.8. In the language of Definition 5.4.7, Lemma 5.4.6 Part (i) states that if the height of w is t_2, and if $t_2 \preccurlyeq t_3$, then the height of $w^{t_2^{-1}t_3}$ is t_3. Further, the leading summand of $w^{t_2^{-1}t_3}$ is $\mu(w) \otimes t_3$.

The formulation in Remark 5.4.8 leads to an important technical point.

Proposition 5.4.9. *Let M be a submodule of W. Then M has a generating set X with the following property: No subset Y of X, whose image $\tau(Y)$ in $\mathcal{T}$ is a chain with respect to the partial order $\preccurlyeq$, can have more than*

$$\min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')} + am, \chi\right\}$$

elements, where $\chi = \chi(K, V^*)$ denotes the number of orbits of K on the nonzero elements of V.

Before proving Proposition 5.4.9, we need a preliminary lemma.

Lemma 5.4.10. *A K'-composition series for V contains at most am factors isomorphic to the trivial module.*

Proof. Let $Q \leq K'$ such that Q^V is semisimple and $\chi(Q^{\Omega_1}, \Omega_1) = m$. By Theorem

2.2.4,

$$V\downarrow_Q = \left(U\uparrow_{H_1}^H\right)\downarrow_Q \cong \bigoplus_{i=1}^{m} U_{x_i}, \tag{5.4.1}$$

where $U_{x_i} := (U\otimes x_i)\uparrow_{Q\cap H_1^{x_i}}^Q$, $\dim U_{x_i} = \dim U = a$, for each i, and $\sum_j |Q : Q\cap H_1^{x_i}| = |H : H_1| = d$. Since Q^V is semisimple, the number of Q-composition factors of $U_{x_i} = (U\otimes x_i)\uparrow_{Q\cap H_1^{x_i}}^Q$ isomorphic to the trivial module 1_Q is precisely

$$\dim \mathrm{Hom}_{\mathbb{F}[Q]}((U\otimes x_i)\uparrow_{Q\cap H_1^{x_i}}^Q, 1_Q) = \dim \mathrm{Hom}_{\mathbb{F}[Q\cap H_1^{x_i}]}((U\otimes x_i), 1_{Q\cap H_1^{x_i}}),$$

applying Theorem 2.2.5. This is at most $\dim(U\otimes x_i) = \dim U = a$. The result now follows immediately from (5.4.1). □

Proof of Proposition 5.4.9. Set $e := \frac{ad-am}{R_{\mathbb{F}}(K')} + am$, and let X be a finite generating set for M, consisting of non-zero elements. Suppose that $Y := \{w_0, w_1, \ldots, w_e\}$ is a subset of X whose image under τ forms a chain in $\mathcal{T}$: Say $\tau(w_0) \preccurlyeq \tau(w_1) \preccurlyeq \ldots \preccurlyeq \tau(w_e)$.

Consider now the vectors $\mu(w_0)$, $\mu(w_1)$, …, $\mu(w_e)$: For $1 \le i \le e+1$ let W_i denote the K'-module generated by $\mu(w_0)$, …, $\mu(w_{i-1})$, and consider the series of K'-modules

$$0 =: W_0 \le W_1 \le \ldots \le W_{e+1} \tag{5.4.2}$$

Suppose that $W_i < W_{i+1}$ for all i. Then the series (5.4.2) can be extended to give a K'-composition series for V. Thus, Lemma 5.4.10 implies that at most am of the factors W_{i+1}/W_i are trivial. Furthermore, the rest have dimension at least $R_{\mathbb{F}}(K')$. It follows that $\dim W_{e+1} = \sum_{i=1}^{e+1} \dim W_i/W_{i-1} \ge am + (e+1-am)R_{\mathbb{F}}(K') > ad$, which is a contradiction, since $\dim V = ad$.

Thus, we must have $\mu(w_i) \in W_i$ for some i. In this case,

$$\mu(w_i) = \sum_{j=0}^{i-1}\sum_{k\in K'} \lambda_{j,k}\mu(w_j)^k,$$

for some scalars $\lambda_{j,k}$. Moreover, the element

$$x := \sum_{j=0}^{i-1}\sum_{k\in K'} \lambda_{j,k} w_j^{k^{\tau(w_j)}\tau(w_j)^{-1}\tau(w_i)}$$

of M has the same leading summand as w_i, by Lemma 5.4.6 Part (i) (see also Remark 5.4.8). Hence, either $x = w_i$ and w_i may be removed from X, or w_i may be replaced in X by the element $w_i - x$, which has height strictly preceding w_i in the full order $\leqslant$. In this way, the resulting (modified) set X still generates M. This procedure can only be carried out a finite number of times, and when it can no longer be repeated, the (modified) generating set can have no more than e elements.

If $\chi \geq e$, then we are done, so assume that $\chi < e$. Let v and w be elements of X whose images $\tau(v)$ and $\tau(w)$ are comparable (with respect to $\preccurlyeq$) in $\mathcal{T}$: Say $\tau(v) \preccurlyeq \tau(w)$. Suppose that $\mu(w)$ and $\mu(v)$ lie in the same K-orbit of V, and let $g \in K$ such that $\mu(w)^g = \mu(v)$. Since K is normal in G, the leading summand of w^g is $\mu(v) \otimes \tau(w)$. Thus, by replacing w with w^g, we may assume that $\mu(v) = \mu(w)$. Then, using Lemma 5.4.6 Part (i) again, we see that $v^{\tau(v)^{-1}\tau(w)}$ has the same leading summand as w. Write $v^{\tau(v)^{-1}\tau(w)} = x + \mu(v) \otimes \tau(w)$, and $w = y + \mu(v) \otimes \tau(w)$, for x, $y \in V$, and let $u = y - x$. Then, we see that, as in the proof of [8, Lemma 5.2], either $u = 0$, and $w = v^{\tau(v)^{-1}\tau(w)}$ may be omitted from X, or $u \neq 0$, and $w = u + v^{\tau(v)^{-1}\tau(w)}$ may be replaced in X by the element u, which has height strictly preceding $\tau(w)$ in the full order $\leqslant$. This way, the resulting set obtained from X still generates M. The procedure outlined above can only be carried out a finite number of times, and when it can no longer be repeated, the (modified) generating set can contain no more than χ elements. This completes the proof. $\square$

Before proving Theorem 5.4.4, we note the following easy consequence of Dilworth's Theorem ([20, Theorem 1.1]):

Lemma 5.4.11. *If a partially ordered set P has no chain of cardinality greater than k, and no antichain of cardinality greater than l, then P cannot have cardinality greater than kl.*

Proof of Theorem 5.4.4. Let $\mathcal{T}$ be a right transversal for H in G with full and partial orders $\leqslant$ and $\preccurlyeq$, as in Lemma 5.4.6. Now define a partial order on the elements of W as follows: First, for each $t \in \mathcal{T}$, choose a full order on the elements of W of height t. Now, for w_1 and w_2 in W, say that $w_1 < w_2$ if $\tau(w_1)$ is less than $\tau(w_2)$ in $(\mathcal{T}, \preccurlyeq)$, or if $\tau(w_1) = \tau(w_2)$ but w_1 precedes w_2 in the full order chosen for elements of height $\tau(w_1)$.

Then $\tau : W \to \mathcal{T}$ is a poset homomorphism which takes incomparable elements to incomparable elements, so no antichain of its domain can have cardinality greater than $\widetilde{\omega}(s)$, by Lemmas 5.2.1 and 5.4.6 Part (ii). Let X be a generating

set for M with the properties guaranteed by Proposition 5.4.9. Then no chain in X can have more than $\min\{\frac{ad-am}{R_{\mathbb{F}}(K')}+am,\chi\}$ elements. Lemma 5.4.11 then implies that

$$|X| \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')}+am,\chi\right\}\widetilde{\omega}(s) \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')}+am,\chi\right\}\left\lfloor\frac{bs}{\sqrt{\log s}}\right\rfloor,$$

where the second inequality follows from Corollary 5.2.3. If $s=p^t$ for p prime, then

$$|X| \leq \min\left\{\frac{ad-am}{R_{\mathbb{F}}(K')}+am,\chi\right\}\left\lfloor\frac{bp^t}{\sqrt{\log t(p-1)}}\right\rfloor,$$

again by Lemma 5.4.11 and Corollary 5.2.3. This completes the proof. □

5.4.2 Induced modules for finite groups: The general case

In this section, we prove a weaker form of Theorem 5.4.4 for general finite groups (i.e. those G for which G^Ω does not necessarily contain a soluble transitive subgroup). We retain the notation introduced at the beginning of Section 5.4.

We begin with a definition. Recall the definitions of $\widetilde{\omega}(s)$, s_p, and $\mathrm{lpp}\,(s)$ from Definitions 1.3.2 and 2.4.1.

Definition 5.4.12. For a prime p, set

$$E(s,p) := \min\left\{\left\lfloor\frac{bs}{\sqrt{(p-1)\log_p s_p}}\right\rfloor, \frac{s}{\mathrm{lpp}\,(s/s_p)}\right\} \text{ and } E_{sol}(s,p) := \min\{\widetilde{\omega}(s), s_p\}$$

where we take $\left\lfloor bs/\sqrt{(p-1)\log_p s_p}\right\rfloor$ to be ∞ if $s_p = 1$.

Proposition 5.4.13. *Let p be prime. Then $E_{sol}(s,p) \leq E(s,p)$.*

Proof. By Corollary 5.2.3 we have $\widetilde{\omega}(s) \leq \left\lfloor\frac{bs}{\sqrt{(p-1)\log_p s_p}}\right\rfloor$. Also, it is clear that $s_p \leq \frac{s}{\mathrm{lpp}\,(s/s_p)}$. The result follows. □

Remark 5.4.14. For any finite group G and any G-module M, $d_G(M)$ is bounded above by $\chi(G,M^*)$.

For the remainder of this section, we will make a further assumption: that the field $\mathbb{F}$ has characteristic $p>0$. We are now ready to state and prove the main result of this section.

Theorem 5.4.15. *For a prime $q \neq p$, let P_q be a Sylow q-subgroup of G. Also, let P' be a maximal p'-subgroup of G. Let M be a submodule of the induced module $W = V \uparrow_H^G$.*

(i) If G is soluble, then

$$d_G(M) \leq \min\left\{\frac{ad - a\chi(P' \cap K, \Omega_1)}{R_{\mathbb{F}}(P' \cap K)} + a\chi(P' \cap K, \Omega_1), \chi(P' \cap K, V^*)\right\} s_p.$$

(ii) Let N be a subgroup of G such that N^Ω is soluble, and let s_i, $1 \leq i \leq t$, be the sizes of the orbits of N on Ω. Then

(a) We have

$$\begin{aligned} d_G(M) \leq \min\Bigg\{&\frac{ad - a\chi(N \cap P' \cap K, \Omega_1)}{R_{\mathbb{F}}(N \cap P' \cap K)} + a\chi(N \cap P' \cap K, \Omega_1), \\ &\chi(N \cap P' \cap K, V^*)\Bigg\} \times \sum_{i=1}^{t} \widetilde{\omega}(s_i). \end{aligned}$$

(b) If N is soluble, and P'_N is a p-complement in N, then

$$\begin{aligned} d_G(M) \leq \min\Bigg\{&\frac{ad - a\chi(P'_N \cap K, \Omega_1)}{R_{\mathbb{F}}(P'_N \cap K)} + a\chi(P'_N \cap K, \Omega_1), \\ &\chi(P'_N \cap K, V^*)\Bigg\} \times \sum_{i=1}^{t} E_{sol}(s_i, p). \end{aligned}$$

(iii) $d_G(M) \leq \min\left\{\frac{ad - a\chi(P_q \cap K, \Omega_1)}{R_{\mathbb{F}}(P_q \cap K)} + a\chi(P_q \cap K, \Omega_1), \chi(P_q \cap K, V^*)\right\} s/s_q.$

(iv) Assume that $s_p > 1$. Then

$$d_G(M) \leq \min\left\{\frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi(K, V^*)\right\} \left\lfloor \frac{bs}{\sqrt{\log s_p}} \right\rfloor.$$

Proof. The proof is based on the idea of Lucchini et al. used in the proof of [37, Lemma 4]. Let Q be a subgroup of G, and choose a full set $\{x_1, x_2, \ldots, x_t\}$ of representatives for the (H, Q)-double cosets in G. Also, for $1 \leq i \leq t$, put $s_i := |Q : Q \cap H^{x_i}|$ (note that, by H^{x_i}, we mean, as usual, the conjugate subgroup

$x_i^{-1}Hx_i$). By Theorem 2.2.4 we have

$$W\downarrow_Q = (V\uparrow_H^G)\downarrow_Q = \bigoplus_{i=1}^{t} V_{x_i} \tag{5.4.3}$$

where $V_{x_i} \cong (V\otimes x_i)\uparrow_{Q\cap H^{x_i}}^{Q}$. Comparing dimensions of the left and right hand side of (5.4.3) above, we get

$$ads = \dim W = \sum_{i=1}^{t} ad|Q : Q\cap H^{x_i}| = ad\sum_{i=1}^{t} s_i$$

so that $\sum_{i=1}^{t} s_i = s$. Clearly, the s_i represent the sizes of the orbits of Q on the right cosets of H in G.

Next, for $1 \le i \le t$, set $V_i := V_{x_1} \oplus V_{x_2} \oplus \ldots \oplus V_{x_i}$. Then, we have a chain $0 = V_0 \le V_1 \le \ldots \le V_t = W$ of Q-submodules of W. This allows us to define the chain of Q-modules $0 = M_0 \le M_1 \le \ldots \le M_t = M$, where $M_i := M \cap V_i$. Furthermore, in this case, the quotient M_i/M_{i-1} is (isomorphic to) a Q-submodule of V_{x_i}. Hence

$$d_G(M) \le d_Q(M) \le \sum_{i=1}^{t} d_Q(M_i/M_{i-1}). \tag{5.4.4}$$

Note that $V\otimes x_i$ is isomorphic to an induced module $(U\otimes x_i)\uparrow_{H_1^{x_i}}^{H^{x_i}}$. Hence, Theorem 2.2.4 implies that $(V\otimes x_i)\downarrow_{Q\cap K}$ is isomorphic to a direct sum

$$(V\otimes x_i)\downarrow_{Q\cap K} \cong \bigoplus_{j} U_{x_{i,j}}, \tag{5.4.5}$$

where $U_{x_{i,j}} \cong (U\otimes x_{i,j})\uparrow_{Q\cap K\cap H_1^{x_{i,j}}}^{Q\cap K}$ is an induced module for $Q\cap K$, and $\sum_j |Q\cap K : Q\cap K\cap {H_1}^{x_{i,j}}| = |H^{x_i} : H_1^{x_i}| = d$.

Suppose that $(|Q|, p) = 1$. Then each V_{x_i} is a semisimple $\mathbb{F}[Q]$-module, so

$$\begin{aligned}
d_Q(M_i/M_{i-1}) &\leq d_Q(V_{x_i}) \\
&\leq d_{Q\cap H^{x_i}}(V \otimes x_i) \\
&\leq d_{Q\cap K}(V \otimes x_i) \\
&\leq \sum_j d_{Q\cap K} U_{x_{i,j}} \\
&\leq \sum_j \min\left\{ \frac{a|Q\cap K : Q\cap K\cap H_1^{x_{i,j}}| - a}{R_{\mathbb{F}}(Q\cap K)} + a, \chi(Q\cap K, \right. \\
&\left. [U_{x_{i,j}}]^*) \right\} \\
&\leq \min\left\{ \sum_j \frac{a|Q\cap K : Q\cap K\cap H_1^{x_{i,j}}| - a}{R_{\mathbb{F}}(Q\cap K)} + a, \sum_j \chi(Q\cap K, \right. \\
&\left. [U_{x_{i,j}})]^*) \right\} \\
&= \min\left\{ \frac{ad - a\chi(Q\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap K)} + a\chi(Q\cap K, \Omega_1), \chi(Q\cap K, V^*) \right\}
\end{aligned}$$

The fourth inequality above follows from (5.4.5), while the fifth follows from Corollary 5.3.6 and Remark 5.4.14. Thus

$$d_G(M) \leq \min\left\{ \frac{ad - a\chi(Q\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap K)} + a\chi(Q\cap K, \Omega_1), \chi(Q\cap K, V^*) \right\} t \quad (5.4.6)$$

by (5.4.4).

Write $s_p := p^\beta$ and $s_q := q^\alpha$. Also, write $s = p^\beta q^\alpha k$ and $|H| = p^\delta q^\gamma l$, where $|H|_p = p^\delta$, $|H|_q = q^\gamma$. We are now ready to prove the theorem.

(i) Suppose that G is soluble, and take $Q := P'$ to be a p-complement in G. Then $|Q| = q^{\alpha+\gamma}kl$. Hence, $s_i = |Q : Q\cap H^{x_i}| \geq q^\alpha k = s/s_p$. Part (i) now follows from (5.4.6), since $s = \sum_{i=1}^t s_i \geq ts/s_p$.

(ii) Take $Q := N$. By Theorem 5.4.4, we have

$$\begin{aligned}
d_Q(M_i/M_{i-1}) \leq \min\left\{ \frac{ad - a\chi(Q\cap P'\cap K, \Omega_1)}{R_{\mathbb{F}}(Q\cap P'\cap K)} + a\chi(Q\cap P'\cap K, \Omega_1), \right. \\
\left. \chi(Q\cap P'\cap K, V^*) \right\} \widetilde{\omega}(s_i).
\end{aligned}$$

Part (a) of (ii) now follows from (5.4.4). Next, assume that N is soluble, with a p-complement P'_N. Then

$$d_Q(M_i/M_{i-1}) \leq \min\left\{ \frac{ad - a\chi(Q \cap P' \cap K, \Omega_1)}{R_{\mathbb{F}}(Q \cap P' \cap K)} + a\chi(Q \cap P' \cap K, \Omega_1), \right.$$
$$\left. \chi(Q \cap P' \cap K, V^*) \right\} (s_i)_p$$

by Part (i). Also, $P'_N = N \cap P'$ for some maximal p'-subgroup P' of G, so Part (b) follows from (5.4.4) by combining the above with Part (ii)(a).

(iii) In the general case, take $Q := P_q$. Then $|Q| = q^{\alpha+\gamma}$, so $s_i = |Q : Q \cap H^{x_i}| \geq q^\alpha$. Also, $s = \sum_{i=1}^t s_i \geq tq^\alpha = ts_q$. Part (iii) then follows from (5.4.6).

(iv) Here, we have $\beta > 0$ since $s_p > 0$. Let P be a Sylow p-subgroup of G, and set $Q = KP$. Then $s_i = |Q : Q \cap H^{x_i}| = |QH^{x_i}|/|H^{x_i}| \geq |PH^{x_i}|/|H^{x_i}| = |P : P \cap H^{x_i}| \geq p^\beta$, for each i. Since $K \leq \mathrm{core}_Q(Q \cap H^{x_i})$, we have $\chi(\mathrm{core}_Q(Q \cap H^{x_i}), (V \otimes x_i)^*) \leq \chi(K, V^*) =: \chi$ for each i. Then (5.4.4) and Theorem 5.4.4 give

$$\begin{aligned} d_G(M) &\leq \sum_{i=1}^t \min\left\{ \frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi \right\} \left\lfloor \frac{bs_i}{\sqrt{\log s_i}} \right\rfloor \\ &\leq \sum_{i=1}^t \min\left\{ \frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi \right\} \left\lfloor \frac{bs_i}{\sqrt{\beta}} \right\rfloor \\ &\leq \min\left\{ \frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi \right\} \left\lfloor \sum_{i=1}^t \frac{bs_i}{\sqrt{\beta}} \right\rfloor \\ &= \min\left\{ \frac{ad - am}{R_{\mathbb{F}}(K')} + am, \chi \right\} \left\lfloor \frac{bs}{\sqrt{\beta}} \right\rfloor \end{aligned}$$

This proves (iv).

□

Since $\frac{ad-f}{e} + f \leq ad$ for positive integers e and f, the following corollary is immediate.

Corollary 5.4.16. *Let M be a submodule of W. Also, let q, P_q and P' be as in Theorem 5.4.15. Then*

(i) If G is soluble, then $d_G(M) \leq \min\{ad, \chi(P' \cap K, V^*)\}\, s_p$.

(ii) Let N be a subgroup of G such that N^Ω is soluble, and let s_i, $1 \leq i \leq t$, be the sizes of the orbits of N on Ω. Then

(a) We have $d_G(M) \leq \min\{ad, \chi(N \cap P' \cap K, V^*)\} \sum_{i=1}^t \widetilde{\omega}(s_i)$.

(b) If N is soluble, and P'_N is a p-complement in N, then

$$d_G(M) \leq \min\left\{ad, \chi(P'_N \cap K, V^*)\right\} \sum_{i=1}^t E_{sol}(s_i, p).$$

(iii) $d_G(M) \leq \min\{ad, \chi(P_q \cap K, V^*)\}\, s/s_q$.

(iv) $d_G(M) \leq \min\{ad, \chi(K, V^*)\} \left\lfloor \frac{bs}{\sqrt{\log s_p}} \right\rfloor$.

We also record the following, which is an immediate consequence of Corollary 5.4.16.

Corollary 5.4.17. *Define E' to be E_{sol} if G^Ω contains a soluble transitive subgroup, and $E' := E$ otherwise. Let M be a submodule of W. Then $d_G(M) \leq adE'(s,p)$.*

Using the definition of $E(s,p)$, and Lemma 2.4.2, we also deduce the following.

Corollary 5.4.18. *Let M be a submodule of W, and fix $0 < \alpha < 1$.*

(i) If $s_p \geq s^\alpha$, then $d_G(M) \leq adE(s,p) \leq ad \left\lfloor \frac{bs\sqrt{\frac{1}{\alpha}}}{\sqrt{\log s}} \right\rfloor$;

(ii) If $s_p \leq s^\alpha$, then $d_G(M) \leq adE(s,p) \leq ad \left\lfloor \frac{\frac{1}{1-\alpha} s}{c' \log s} \right\rfloor$;

(iii) We have

$$d_G(M) \leq adE(s,p) \leq \begin{cases} \left\lfloor \frac{2ads}{c' \log s} \right\rfloor, & \text{if } 2 \leq s \leq 1260, \\ \left\lfloor \frac{adbs\sqrt{2}}{\sqrt{\log s}} \right\rfloor, & \text{if } s \geq 1261. \end{cases}$$

Proof. Part (i) follows immediately from the definition of $E(s,p)$, while Part (ii) follows from the definition and Lemma 2.4.2. Finally, set $\alpha := 1/2$. Then

$$\frac{2ads}{c' \log s} \leq \frac{adbs\sqrt{2}}{\sqrt{\log s}}$$

for $s \geq 1261$, so Part (iii) also follows. □

The following is also immediate, from Part (ii) of Theorem 5.4.15.

Corollary 5.4.19. *Let M be a submodule of W. If G contains a soluble subgroup N, acting transitively on Ω, then*

$$d_G(M) \leq \min\left\{\frac{ad - a\chi(P'_N \cap K, \Omega_1)}{R_{\mathbb{F}}(P'_N \cap K)} + a\chi(P'_N \cap K, \Omega_1), \chi(P'_N \cap K, V^*)\right\} \times E(s,p)$$

where P'_N is a p-complement in N.

5.5 An application to induced modules for bottom heavy groups

The proofs of the main results of this thesis will usually only require the bounds on $d_G(M)$ from Corollary 5.4.16. For a specific case of the proof of Theorem 1.2.3 however, we will need the stronger bounds provided by Theorem 5.4.15. This case is the 'bottom heavy case', which we will now define. Throughout, we retain the notation introduced at the beginning of Section 5.4. In particular, H is a subgroup of G of index of index $s \geq 2$, H_1 is a subgroup of H of index $d \geq 1$, Ω is the set of right cosets of H in G, Ω_1 is the set of right cosets of H_1 in H, and $K := \mathrm{Ker}_G(\Omega)$. Note that we also continue to assume that the field $\mathbb{F}$ has characteristic $p > 0$.

Definition 5.5.1. Assume that K^{Ω_1}, viewed as a subgroup of $\mathrm{Sym}\,(d)$, contains $\mathrm{Alt}(d)$. Then we say that the triple (G, H, H_1) is *bottom heavy*.

Before stating the main rsult of this section, we introduce Vinogradov notation: we will write

$$A \ll B$$

to mean $A = O(B)$. The main result can now be stated as follows.

Proposition 5.5.2. *Assume that $d \geq 5$ and that (G, H, H_1) is bottom heavy. Let M be a submodule of W. Then*

(i) $d_G(M) \leq 2as$, and;

(ii) If $s_p > 1$, then $d_G(M) \ll \frac{as}{\sqrt{\log s_p}}$.

Before proving Proposition 5.5.2, we require the following:

Proposition 5.5.3. *Assume that (G, H, H_1) is bottom heavy and that $d \geq 5$. Choose K' to be a subgroup of K minimal with the property that $K'^{\Omega_1} \cong \mathrm{Alt}(d)$. Then a K'-composition series for $V\downarrow_{K'}$ has at most $2a$ factors isomorphic to the trivial K'-module.*

Proof. By the minimality of K', we have $C := \mathrm{core}_H(H_1) \cap K' \leq \Phi(K')$, and hence C is soluble. Let E be a subgroup of K' containing C such that E/C is soluble and, viewed as a subgroup of $\mathrm{Sym}\,(d)$, has at most two orbits, such that each orbit is of p'-length (such a subgroup exists by Lemma 5.3.8). Then E is soluble, so we may choose a p-complement F in E. Then $F/F \cap C$ also has at most two orbits (and each F-orbit has p'-length).

Next, consider the F-module $X := V\downarrow_F \cong U\uparrow_{H_1}^H\downarrow_F$. Since $F \leq K'$, it suffices to prove that X has at most $2a$ trivial composition factors. To see this, note that since F has at most two orbits on Ω_1 (i.e. the cosets of H_1 in H), represented by x_1 and x_2, say, Theorem 2.2.4 yields

$$X \cong X_1 \oplus X_2 \text{ or } X \cong X_1$$

where $X_i \cong (U \otimes x_i)\uparrow_{F\cap H_1^{x_i}}^F$. Now, since F has p'-order, X_i is a semisimple F-module. Hence, the number of trivial factors in an F-composition series for X_i is precisely the number of trivial summands of X_i, which is

$$\dim \mathrm{Hom}_{\mathbb{F}[F]}(X_i, 1_F),$$

where 1_F denotes the trivial F-module. By Theorem 2.2.5, this is equal to

$$\dim \mathrm{Hom}_{\mathbb{F}[F\cap H_1^{x_i}]}(U\downarrow_{F\cap H_1^{x_i}}, 1_{F\cap H_1^{x_i}}) \leq \dim U = a.$$

The claim follows. □

Proof of Proposition 5.5.2. Choose K' to be a subgroup of K minimal with the property that $K'^{\Omega_1} \cong \mathrm{Alt}(d)$. Then

$$\mathrm{core}_H(H_1) \cap K' \leq \Phi(K'). \tag{5.5.1}$$

Hence, since

$$\mathrm{Alt}(d) \cong K'^{\Omega} \cong K'/\mathrm{core}_H(H_1) \cap K',$$

Proposition 5.3.7 applies: $R_{\mathbb{F}}(K') \geq \overline{R}(\mathrm{Alt}(d))$. Note also that $m \leq 2$ by Lemma

5.3.8. Since $d \ll \overline{R}(\mathrm{Alt}(d))$ (see [29, Proposition 5.3.7]), Part (ii) now follows from Theorem 5.4.15 Part (iv).

We now prove (i). It follows from Lemma 5.3.8 that K' has a subgroup N such that N^{Ω_1} is soluble and has at most 2 orbits. Furthermore, each orbit has p'-length. Also, N is soluble, by (5.5.1).

We now want to apply Corollary 5.4.16 Part (ii)(b), with (G, H, H_1, V, Ω) replaced by $(H, H_1, H_1, U, \Omega_1)$ (also, (a, s, d) is replaced by $(a, d, 1)$): let d_i, for $i \leq 2$, denote the lengths of the N^{Ω_1} orbits. Then

$$E_{sol}(d_i, p) \leq (d_i)_p = 1,$$

so $E_{sol}(d_i, p) = 1$. Hence for each H-submodule M' of the induced module $V = U \uparrow_{H_1}^{H}$, we have

$$d_H(M') \leq a \sum_{i=1}^{t} E_{sol}(d_i, p) \leq 2a.$$

Since M is a submodule of

$$U \uparrow_{H_1}^{G} \cong V \uparrow_{H}^{G} \cong \sum_{i=1}^{s} V \otimes t_i$$

where (see Definition 2.2.2) each $V \otimes t_i$ is isomorphic, as an H-module, to V, the result now follows. □

Chapter 6

Minimal generation of transitive permutation groups

6.1 Introduction

In this chapter, we state and prove the second main result of this thesis, which is stated as Theorem 1.2.2 in Chapter 1. The theorem follows in the primitive case from Theorem 2.1.15, so this chapter deals predominantly with the case when $G \leq \mathrm{Sym}(n)$ is imprimitive. In this case, G is a large subgroup of a wreath product $R \wr S$, where R is primitive of degree $r \geq 2$, S is transitive of degree $s \geq 2$, and $n = rs$. Due to the nature of our bounds, the most difficult cases to deal with are when $R = \mathrm{Sym}(2)$ or $R = \mathrm{Sym}(4)$, i.e. when G has a minimal block of cardinality either 2 or 4. (Essentially, this is because Sym(2) and Sym(4) have large composition lengths relative to their degree.) We deal with the Sym(4) case in Corollary 6.2.8; the idea being that we can use the transitive action of the Sylow 3-subgroup in Sym(4) on the non-identity elements of the Klein 4-group $V \trianglelefteq \mathrm{Sym}(4)$ to reduce the contribution of V to our bounds (this is the primary reason we include the invariant χ in our bounds in Chapter 4).

However, no such option is available to us when $R \cong \mathrm{Sym}(2)$, since Sym(2) is abelian. If G has another minimal block, of cardinality larger than 2, then we can avoid the problem by using this block instead. However, we cannot do this if all minimal blocks for G have cardinality 2, so assume that this is the case. Then, as we will prove in Section 5.2 below, we have $d(G) \leq E(s, 2) + d(S)$. Now, since we just need to bound $d(S)$, we apply the same methods to the transitive group $S \leq \mathrm{Sym}(s)$.

Apart from finitely many cases, our methods yield the upper bound we want: the only problems occur when we "repeatedly get" blocks of cardinality 2. This is encapsulated in the following non-standard definition.

Definition 6.1.1. Let G be a transitive permutation group, and let

$$X := (R_1, R_2, \ldots, R_t)$$

be a tuple of primitive components for G, where each R_i has degree $r_i \geq 2$. Define

$$\begin{aligned} \mathrm{bl}_{X,2}(G) &:= \min\{i : r_i \neq 2\} - 1, \text{ and} \\ \mathrm{bl}_2(G) &:= \min\{\mathrm{bl}_{X,2}(G) : X \text{ a tuple of primitive components for } G\}. \end{aligned}$$

We call $\mathrm{bl}_2(G)$ the 2-*block number* of G.

Alternatively, the 2-block number of a transitive permutation group G can be defined inductively as follows: if G is primitive, or if G is imprimitive with a minimal block of cardinality greater than 2, then set $\mathrm{bl}_2(G) := 0$. Otherwise, G is imprimitive and all minimal blocks for G have cardinality 2. Let Δ be such a minimal block, and let $\Gamma := \{\Delta^g : g \in G\}$ be the set of G-translates of Δ. Also, let $K := \mathrm{Ker}_G(\Gamma)$. Then define $\mathrm{bl}_2(G) := 1 + \mathrm{bl}_2(G/K)$.

For example, a transitive 2-group G of degree 2^k will have $\mathrm{bl}_2(G) = k$. In other words, any tuple of primitive components for G will consist entirely of Sym(2)s. This is because for any prime p, any minimal block of any transitive p-group has cardinality p.

Remark 6.1.2. If $\mathrm{bl}_2(G) \geq 1$, then G has a block of size $2^{\mathrm{bl}_2(G)}$, by Remark 2.1.8.

We can now restate Theorem 1.2.2 more precisely as follows.

Theorem 6.1.3. *Let G be a transitive permutation group of degree $n \geq 2$. Then*

(1) $d(G) \leq \left\lfloor \frac{cn}{\sqrt{\log n}} \right\rfloor$, *where* $c := 1512660\sqrt{\log(2^{19}15)}/(2^{19}15) = 0.920581\ldots$.

(2) $d(G) \leq \left\lfloor \frac{c_1 n}{\sqrt{\log n}} \right\rfloor$, *where* $c_1 := \sqrt{3}/2 = 0.866025\ldots$, *unless each of the following conditions hold:*

(i) $n = 2^k v$, *where* $v = 5$ *and* $17 \leq k \leq 26$, *or* $v = 15$ *and* $15 \leq k \leq 35$;

(ii) G contains no soluble transitive subgroups; and

(iii) $\mathrm{bl}_2(G) \geq f$, *where* f *is specified in the middle column of Table A.2 (see Appendix A).*

In these exceptional cases, the bounds for $d(G)$ *in Table A.2 hold.*

Recall that by "log", we always mean log to the base 2. The following is immediate from Theorem 6.1.3.

Corollary 6.1.4. *Let* G *be a transitive permutation group of degree* n*, containing a soluble transitive subgroup. Then*

$$d(G) \leq \left\lfloor \frac{c_1 n}{\sqrt{\log n}} \right\rfloor,$$

where $c_1 = \sqrt{3}/2$.

As can be seen from the proof of Theorem 6.1.3, and the statement of the theorem itself, the cases when $\mathrm{bl}_2(G)$ is large are the most difficult to deal with using our methods. We believe that the finite number of exceptions given in Theorem 6.1.3 Part (2) are not exceptions at all, that is, we believe that the bound $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$ should hold for all n and all G.

Note also that, as shown in [28], the bounds in our results are of the right order. Moreover, the infimum of the set of constants $\bar{c}$ satisfying $d(G) \leq \bar{c}n/\sqrt{\log n}$, for all soluble transitive permutation groups G of degree $n \geq 2$, is the constant c_1 in Theorem 6.1.3, since $d(G) = 4$ when $n = 8$ and $G \cong D_8 \circ D_8$. We conjecture that the best "asymptotic" bound, that is, the best possible upper bound when one is permitted to exclude finitely many cases, is $d(G) \leq \lfloor \widetilde{c}n/\sqrt{\log n} \rfloor$, where $\widetilde{c}$ is some constant satisfying $b/2 \leq \widetilde{c} < b = \sqrt{2/\pi}$ (see Example 6.3.2 for more details).

In Section 6.2 we discuss an application of the results of Chapter 4 to wreath products. We reserve Section 6.3 for the proof of Theorem 6.1.3.

6.2 Wreath products

We first make the following easy observation.

Proposition 6.2.1. *Let* $A = T_1 \times T_2 \times \ldots \times T_f$*, where each* T_i *is isomorphic to the nonabelian finite simple group* T*. Suppose that* $M \leq A$ *is a subdirect product of* A*, and suppose that* $M' \trianglelefteq M$ *is also a subdirect product of* A*. Then* $M' = M$.

Proof. We prove the claim by induction on f, and the case $f = 1$ is trivial, so assume that $f > 1$. Since M is subdirect, each $M \cap T_i$ is normal in T_i. If $M = A$, then since the only normal subgroups of A are the groups $\prod_{i \in Y} T_i$, for $Y \subseteq \{1, \ldots, f\}$, the result is clear. So assume that $M \cap T_i = 1$ for some i. Then $M' \cap T_i = 1$, and $M'T_i/T_i$ and MT_i/T_i are subdirect products of $\prod_{j \neq i} T_j$. It follows, using the inductive hypothesis, that $M'T_i = MT_i$. Hence $M' = M$, since $M \cap T_i = 1$, and the proof is complete. □

We also need the following result of Lucchini and Menegazzo.

Theorem 6.2.2 (**[32] and [36]**). *Let L be a proper minimal normal subgroup of the finite group G. Then $d(G) \leq d(G/L) + 1$. Furthermore, if L is the unique minimal normal subgroup of G, then $d(G) \leq \max\{2, d(G/L)\}$.*

We will now fix some notation which will be retained for the remainder of the chapter.

- Let R be a finite group (we do not exclude the case $R = 1$).
- Let S be a transitive permutation group of degree $s \geq 2$.
- Let G be a large subgroup of the wreath product $R \wr S$ (see Definition 2.1.7).
- Write $B := R_{(1)} \times R_{(2)} \times \ldots \times R_{(s)}$ for the base group of $R \wr S$.
- write $\pi : G \to S$ for the projection homomorphism onto the top group.
- Let $H := N_G(R_{(1)}) = \pi^{-1}(\mathrm{Stab}_S(1))$.
- Let $\Omega := H\backslash G$.
- Let $K := G \cap B = \mathrm{core}_G(H) = \mathrm{Ker}_G(\Omega)$.

Recall that for a subgroup N of R, $B_N \cong N^s$ denotes the direct product of the distinct S-conjugates of N. In particular, if $N \trianglelefteq R$, then $B_N \trianglelefteq R \wr S$. Throughout, we will view R as a subgroup of B by identifying R with $R_{(1)}$. We also note that

- $|G : H| = s$; and
- $S = G^{\Omega}$.

In particular, the notation is consistent with the notation introduced at the beginning of Section 5.4.

Remark 6.2.3. The results in this section will be obtained by applying the results in Chapter 4 with $H = H_1$ and $d = 1$ (see the notation introduced at the beginning of Section 5.4).

Remark 6.2.4. If R is a transitive permutation group, acting on a set Δ, then G is an imprimitive permutation group acting on the set $\Delta \times \{1, 2, \ldots, s\}$, and $H = \mathrm{Stab}_G((\Delta, 1))$. Furthermore $H^\Delta = R$, since G is large (see Remark 2.1.11).

Our strategy for proving Theorem 6.1.3 can now be summarised as follows:

Step 1: Show that K is "built" from induced modules for G, and non-abelian G-chief factors.

Step 2: Derive bounds on $d(G)$ in terms of the factors from Step 1 and $d(S)$.

Step 3: Use Theorem 6.2.2, together with the results from Chapter 4, to bound the contributions from the factors in Step 1 to the bound from Step 2.

Step 4: Use induction to bound $d(S)$.

We begin with Step 1.

Lemma 6.2.5. *Suppose that $R > 1$ and that $1 := N_0 \leq N_1 \leq \ldots \leq N_e = R$ is a normal series for R, where each factor is either elementary abelian, or a nonabelian chief factor of R. Consider the corresponding normal series $1 := G \cap B_{N_0} \leq G \cap B_{N_1} \leq \ldots \leq G \cap B_{N_e} = G$ for G. Let $V_i := N_i/N_{i-1}$ and $M_i := G \cap B_{N_i}/G \cap B_{N_{i-1}}$.*

(i) If V_i is elementary abelian, then M_i is a submodule of the induced module $V_i \uparrow_H^G$.

(ii) If V_i is a nonabelian chief factor of R, then M_i is either trivial, or a nonabelian chief factor of G.

Proof. Assume first that V_i is elementary abelian, of order p^a say. Then $B_{N_i}/B_{N_{i-1}}$ is a module for G of dimension $as = a|G : H|$ over the finite field of order p. Furthermore, $B_{N_i}/B_{N_{i-1}}$ is generated, as a G-module, by the H-module V_i. It now follows from Proposition 2.2.6 that $B_{N_i}/B_{N_{i-1}}$ is isomorphic to the induced module $V_i \uparrow_H^G$. This proves (i).

Next, suppose that V_i is a nonabelian chief factor of R. Write bars to denote reduction modulo $B_{N_{i-1}}$. Then $\overline{G}$ is a large subgroup of the wreath product $\overline{R} \wr S$, and $\overline{N_i}$ is a nonabelian minimal normal subgroup of $\overline{R}$. So we just need to prove

that $\overline{G} \cap \overline{B_{N_i}}$ is either trivial or a nonabelian minimal normal subgroup of $\overline{G}$. To this end, consider the projection maps

$$\overline{\rho_j} : N_{\overline{G}}(\overline{R_{(j)}}) \to \overline{R_{(j)}}$$

defined in (2.1.1). Suppose that M is a normal subgroup of $\overline{G}$ contained in $\overline{G} \cap \overline{B_{N_i}}$. Then $M \leq N_{\overline{G}}(\overline{R_{(1)}})$, and hence $\overline{\rho_1}(M)$ is a normal subgroup of $\overline{\rho_1}(N_{\overline{G}}(\overline{R_{(1)}})) = \overline{R_{(1)}}$ contained in the minimal normal subgroup of $\overline{R_{(1)}}$ corresponding to $\overline{N_i}$. If $\overline{\rho_1}(M) = 1$ then $\overline{\rho_j}(M) = 1$ for all j, since $\pi(\overline{G}) = S$ is transitive. Hence, in this case, we have $M = 1$. Otherwise, $\overline{\rho_1}(M) \cong \overline{N_i}$, and M is a subdirect product of s copies of $\overline{N_i}$. In this case, since a minimal normal subgroup of a finite group is a direct product of simple groups, we must have $M = \overline{G} \cap \overline{B_{N_i}}$ by Proposition 6.2.1. Thus, if $\overline{G} \cap \overline{B_{N_i}}$ is non-trivial, then $\overline{G} \cap \overline{B_{N_i}}$ is a nonabelian minimal normal subgroup of $\overline{G}$, as required. □

For the remainder of this section, suppose that $1 := N_0 \leq N_1 \leq \ldots \leq N_e = R$ is a chief series for R, and let $V_i := N_i/N_{i-1}$ and $M_i := G \cap B_{N_i}/G \cap B_{N_{i-1}}$. If V_i is abelian we will also write $|V_i| = p_i^{a_i}$, for p_i prime.

We now have Step 2.

Corollary 6.2.6. *We have*

$$d(G) \leq \sum_{V_i \text{ abelian}} d_G(M_i) + c_{nonab}(R) + d(S)$$

Proof. We will prove the corollary by induction on $|R|$. If $|R| = 1$ then the bound is trivial, since $G \cong S$ in that case, so assume that $|R| > 1$, and note that

$$G/M_1 \text{ is a large subgroup of } (R/V_1) \wr S. \tag{6.2.1}$$

Suppose first that V_1 is abelian. Then M_1 is a G-module, so

$$d(G) \leq d_G(M_1) + d(G/M_1).$$

Since $c_{nonab}(R) = c_{nonab}(R/V_1)$, (6.2.1) and the inductive hypothesis give the result.

So we may assume that V_1 is nonabelian. Then M_1 is either trivial or a minimal normal subgroup of G, by Lemma 6.2.5 Part (ii). Hence, $d(G) \leq d(G/M_1) + 1$ by Theorem 6.2.2. The result now follows, again from (6.2.1) and the inductive hypothesis. □

Before stating our next corollary, we refer the reader to Definition 5.4.12 for a reminder of the definitions of the functions E and E_{sol}. The next two corollaries deal with Step 3.

Corollary 6.2.7. *Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Then*

(i) $d(G) \leq \sum_{V_i \text{ abelian}} a_i E'(s, p_i) + c_{nonab}(R) + d(S)$.

(ii) Suppose that $|R| = 2$ and $s = 2^m q$, where q is odd, and that S has a tuple of primitive components $X = (R_2, \ldots, R_t)$, where $\mathrm{bl}_{X,2}(S) \geq 1$. Let Γ be a full set of blocks for S of size $2^{\mathrm{bl}_{X,2}(S)}$, and set $\widetilde{S} := S^\Gamma$. Then

$$d(G) \leq \sum_{i=0}^{\mathrm{bl}_{X,2}(S)} E'(2^{m-i}q, 2) + d(\widetilde{S}).$$

(iii) Suppose that $|R| = 2$ and $s = 2^m 3$, and that S contains no soluble transitive subgroups. Then by Corollary 4.3.7 there exists a Mersenne prime $p_1 = 2^a - 1$ and a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that

(1) $m = ea + t$, and;

(2) There exists a subgroup N of G, such that N^Ω is soluble and has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p_1^k \times 2^{t-t_1}$, for each $0 \leq k \leq e$.

Here, we have

$$d(G) \leq \sum_{k=0}^{e} 2^{t-t_1} \binom{e}{k} E_{sol}(3p_1^k 2^{t_1}, 2) + d(S).$$

Proof. By Corollary 6.2.6, we have

$$d(G) \leq \sum_{V_i \text{ abelian}} d_G(M_i) + c_{nonab}(R) + d(S).$$

Now, by Corollary 5.4.17, $d_G(M_i) \leq E'(s, p_i)$. This proves (i).

To prove (iii) first note that, by Corollary 4.3.7, and as mentioned in the statement of (iii), there exists a Mersenne prime $p_1 := 2^a - 1$, and a triple (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that

(i) $m = ea + t$, and;

(ii) There exists a subgroup N of G, such that N^Ω is soluble and has 2^{e+t_1} orbits, with $\binom{e}{k}2^{t_1}$ of them of length $3p_1^k \times 2^{t-t_1}$, for each $0 \leq k \leq e$.

Note that, since $|R| = 2$, the base group $K \leq R^s$ of G is soluble. Hence, since $N^\Omega \cong N/N \cap K$ is soluble, it follows that N itself is also soluble. Corollary 5.4.16 Part (ii)(b) (with $ad = 1$) then implies that

$$d_G(M_1) \leq \sum_{k=0}^{e} 2^{t_1} \binom{e}{k} E_{sol}(3p_1^k 2^{t-t_1}, 2)$$

Since $|R| = 2$, we have $d(G) \leq d_G(M_1) + d(S)$, and the result follows.

Finally, we prove Part (ii). We will show that

$$d(S) \leq \sum_{i=1}^{\mathrm{bl}_{X,2}(S)} E(2^{m-i}q, 2) + d(\widetilde{S}) \tag{6.2.2}$$

by induction on $\mathrm{bl}_{X,2}(S)$. The result will then follow, since $d(G) \leq E'(2^m q, 2) + d(S)$ by Part (i). Now, by hypothesis, S has a tuple of primitive components $X = (R_2, \ldots, R_t)$. Also, $|R_2| = 2$ since $\mathrm{bl}_{X,2}(S) \geq 1$. Hence, by Theorem 2.1.9, S is a large subgroup of a wreath product $R_2 \wr S_2$, where either $S_2 = 1$, or S_2 is a transitive permutation group of degree $2^{m-1}q$, with a tuple $Y := (R_3, \ldots, R_t)$ of primitive components. If $S_2 = 1$ then the result follows, since $s = 4$ and $\widetilde{S} = 1$ in that case. So assume that $S_2 > 1$. By Part (i), we have

$$d(S) \leq E'(2^{m-1}q, 2) + d(S_2) \tag{6.2.3}$$

If $\mathrm{bl}_{X,2}(S) = 1$ then $S_2 = \widetilde{S}$ and (6.2.2) follows from (6.2.3). So assume that $\mathrm{bl}_{X,2}(S) > 1$. Then $\mathrm{bl}_{Y,2}(S_2) = \mathrm{bl}_{X,2}(S) - 1 \geq 1$. The inductive hypothesis then yields $d(S_2) \leq \sum_{i=1}^{\mathrm{bl}_{Y,2}(S_2)} E(2^{m-1-i}q, 2) + d(\widetilde{S}) = \sum_{i=2}^{\mathrm{bl}_{X,2}(S)} E(2^{m-i}q, 2) + d(\widetilde{S})$. The bound (6.2.2) now follows immediately from (6.2.3), which completes the proof. □

The next corollary will be key in our proof of Theorem 6.1.3 when G is imprimitive with minimal block size 4.

Corollary 6.2.8. *Assume that $R = S_4$ or $R = A_4$. Define E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise. Then*

$$d(G) \leq E'(s, 2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E'(s, 3) + d(S).$$

Proof. Let $\Delta := \{1, 2, 3, 4\}$, so that R is transitive on Δ. We have $V_1 \cong 2^2$, $V_2 \cong 3$, and $V_3 \cong 2$ if $R \cong S_4$. Since K^Δ is a normal subgroup of $H^\Delta = R$ (see Remark 6.2.4), K^Δ is isomorphic to either 2^2, A_4, or S_4. In the first two cases M_3 is trivial, so

$$d(G) \leq d_G(M_1) + d_G(M_2) + d(S) \leq 2E'(s, 2) + E'(s, 3) + d(S)$$

by Corollaries 6.2.6 and 5.4.17. So assume that $K^\Delta \cong S_4$. Then a Sylow 3-subgroup P_3 of K^Δ acts transitively on the non-identity elements of V_1. Thus, $\chi(P_3 \cap K, V_1^*) = 1$, so

$$d_G(M_1) \leq \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\}$$

by Corollary 5.4.16 Parts (iii) and (iv), with $(p, q) := (2, 3)$. The result follows. □

6.3 The proof of Theorem 6.1.3

In this section, we prove Theorem 6.1.3. First, we deal with Step 4: the inductive step. As mentioned in Section 6.1, the cases where $\mathrm{bl}_2(G)$ is large are the most difficult to deal with using our methods. In these cases, we have $d(G) \leq E(s, 2) + d(S)$ and usually the bounds on $d(S)$ which come from the inductive hypothesis then suffice to prove the theorem. However in some small cases the inductive hypothesis does not suffice, and we have to work harder. These cases, of which there are finitely many, are the subject of Appendix A, and include both the exceptional cases from Theorem 6.1.3 (Table A.2), and some additional cases which have a large 2-part (Table A.1). The purpose of Lemma 6.3.1 is to prove that the bounds in Appendix A hold.

Throughout this section, we retain the same notation as introduced immediately following Theorem 6.2.2, with one additional assumption: that R is a primitive permutation group of degree $r \geq 2$. Hence, G is a transitive permutation group of degree $n := rs$, and Remark 6.2.4 applies. Also, set E' to be E_{sol} if S contains a soluble transitive subgroup, and $E' := E$ otherwise.

Recall also that $p_i^{a_i}$ denote the orders of the abelian chief factors of R, for p_i prime.

Lemma 6.3.1. *Assume that Theorem 6.1.3 holds for degrees less than n. Then*

(i) The bounds in Table A.1 (see Appendix A) hold, and;

(ii) If n and f are as in Table A.2, and either

(a) G contains a soluble transitive subgroup; or

(b) $\mathrm{bl}_2(G) < f$,

then $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$, *where* $c_1 = \frac{\sqrt{3}}{2}$.

(iii) If n and f are as in Table A.2, and

(a) G contains no soluble transitive subgroup; and

(b) $\mathrm{bl}_2(G) < f$,

then, the bounds in Table A.2 (Appendix A) hold.

Proof. We first recall some bounds which will be used throughout the proof. We have

$$d(G) \leq s\lfloor \log r \rfloor + d(S), \text{ if } r \geq 4; \text{ and} \tag{6.3.1}$$

$$d(G) \leq \sum_i a_i E'(s, p_i) + c_{nonab}(R) + d(S). \tag{6.3.2}$$

These bounds follow from Corollary 2.1.16 and Corollary 6.2.7 Part (i) respectively.

To bound $d(S)$ above, we use Table B.1 (Appendix B) if $2 \leq s \leq 32$; otherwise, we use either the previous rows of Tables A.1 and A.2; or the bound $d(S) \leq \lfloor c_1 s/\sqrt{\log s} \rfloor$ (from the hypothesis of the lemma) if s is not in Tables A.1 or A.2.

We will first prove (i) and (ii).

(i) and (ii) The values of n occurring in Table A.1 are $n = 2^m$ for $6 \leq m \leq 11$; $n = 2^{m+1}3$ for $3 \leq m \leq 19$; $n = 2^m 5$ for $3 \leq m \leq 16$; and $n = 2^m 15$ for $2 \leq m \leq 14$. We distinguish a number of cases. Recall that $n = rs$. Throughout, we define $E'' := E_{sol}$ if s is of the form $s = 2^m$, and $E'' := E$ otherwise. (Note that a transitive group of prime power degree always contains a soluble transitive subgroup.)

1. $r > 16$. Then $d(G) \leq s\lfloor \log r \rfloor + d(S)$ by (6.3.1). Combining this with the bounds on $d(S)$ described above gives the required for each n in Table A.1, and each possible pair (r, s) with $r > 16$ and $n = rs$, except when $(n, r, s) = (3145728, 24, 131072)$. However, each primitive group of degree 24 is either simple, or has a simple normal subgroup of index 2 (using the MAGMA [6] database). Hence, in this case, (6.3.2), together with the

hypothesis of the lemma, gives $d(G) \leq E(s,2)+1+\lfloor c_1 s/\sqrt{\log s}\rfloor = 52895$. This gives us what we need.

2. $r = 2$. We distinguish two sub-cases.

   (a) S contains a soluble transitive subgroup. Then $d(G) \leq E_{sol}(s,2) + d(S)$ by (6.3.2), and this, together with the bounds on $d(S)$ described above gives the bounds in Table A.1 in each of the relevant cases.

   (b) S contains no soluble transitive subgroups. Then s is not of the form $s = 2^m$. We distinguish each of the relevant cases.

      i $s = 2^m 3$, for some $3 \leq m \leq 19$. By using the MAGMA database [6], we see that each transitive permutation group of degree 24 contains a soluble transitive subgroup, so we must have $s = 2^m 3 \geq 48$. In particular, $4 \leq m \leq 19$. By Corollary 6.2.7 Part (iii) there exists a Mersenne prime $p_1 = 2^a - 1$ and a triple of integers (e, t_1, t), with $e \geq 1$, and $t \geq t_1 \geq 0$, such that $m = ea + t$, and

$$d(G) \leq \sum_{k=0}^{e} 2^{t-t_1} \binom{e}{k} E_{sol}(3p_1^k 2^{t_1}, 2) + d(S). \tag{6.3.3}$$

      Since $4 \leq m \leq 19$, the possibilities for n and the triple (a,e,t) are as follows:

Table 5.1

s	(a,e,t)
48	$(3,1,1)$
96	$(3,1,2)$, $(5,1,0)$
192	$(3,1,3)$, $(3,2,0)$, $(5,1,1)$
384	$(3,1,4)$, $(3,2,1)$, $(5,1,2)$, $(7,1,0)$
768	$(3,1,5)$, $(3,2,2)$, $(5,1,3)$, $(7,1,1)$
1536	$(3,1,6)$, $(3,2,3)$, $(3,3,0)$, $(5,1,4)$, $(7,1,2)$
3072	$(3,1,7)$, $(3,2,4)$, $(3,3,1)$, $(5,1,5)$, $(7,1,3)$, $(5,2,0)$
6144	$(3,1,8)$, $(3,2,5)$, $(3,3,2)$, $(5,1,6)$, $(7,1,4)$, $(5,2,1)$
12288	$(3,1,9)$, $(3,2,6)$, $(3,3,3)$, $(3,4,0)$, $(5,1,7)$, $(7,1,5)$, $(5,2,2)$

Table 5.1 ctd.	
n	(a,e,t)
24576	$(3,1,10)$, $(3,2,7)$, $(3,3,4)$, $(3,4,1)$, $(5,1,8)$, $(7,1,6)$, $(13,1,0)$, $(5,2,3)$
49152	$(3,1,11)$, $(3,2,8)$, $(3,3,5)$, $(3,4,2)$, $(5,1,9)$, $(7,1,7)$, $(13,1,1)$, $(5,2,4)$, $(7,2,0)$
98304	$(3,1,12)$, $(3,2,9)$, $(3,3,6)$, $(3,4,3)$, $(3,5,0)$, $(5,1,10)$, $(7,1,8)$, $(13,1,2)$, $(5,2,5)$, $(7,2,1)$, $(5,3,0)$
196608	$(3,1,13)$, $(3,2,10)$, $(3,3,7)$, $(3,4,4)$, $(3,5,1)$, $(5,1,11)$, $(7,1,9)$, $(13,1,3)$, $(5,2,6)$, $(7,2,2)$, $(5,3,1)$

Table 5.1 ctd.	
s	(a,e,t)
393216	$(3,1,14)$, $(3,2,11)$, $(3,3,8)$, $(3,4,5)$, $(3,5,2)$, $(5,1,12)$, $(7,1,10)$, $(13,1,4)$, $(17,1,0)$, $(5,2,7)$, $(7,2,3)$, $(5,3,2)$
786432	$(3,1,15)$, $(3,2,12)$, $(3,3,9)$, $(3,4,6)$, $(3,5,3)$, $(3,6,0)$, $(5,1,13)$, $(7,1,11)$, $(13,1,5)$, $(17,1,1)$, $(5,2,8)$, $(7,2,4)$, $(5,3,3)$
1572864	$(3,1,16)$, $(3,2,13)$, $(3,3,10)$, $(3,4,7)$, $(3,5,4)$, $(3,6,1)$, $(5,1,14)$, $(7,1,12)$, $(13,1,6)$, $(17,1,2)$, $(19,1,0)$, $(5,2,9)$, $(7,2,5)$, $(5,3,4)$

Going through each of the relevant values of n in the first column of Table A.1, each triple (a,e,t) in the last column of Table 5.1, and each possible value of $t_1 \leq t$, with $n/2 = 2^{ea+t}3$, the required bound follows from (6.3.3) each time.

ii $s = 2^m5$, for some $2 \leq m \leq 15$; or $s = 2^m15$ for some $1 \leq m \leq 14$. Then the bound $d(G) \leq E(s,2) + d(S)$, together with the bounds on $d(S)$ described above, give the bounds in Table A.1 in each case.

3. $r = 3$. Here, $d(G) \leq E''(s,3) + E''(s,2) + d(S)$, and the bounds from Table A.1 follow in each case from applying the usual upper bounds on $d(S)$.

4. $r = 4$. Then

$$d(G) \leq E''(s,2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E''(s,3) + d(S) \qquad (6.3.4)$$

by Corollary 6.2.8. Combining this with the bounds on $d(S)$ described above again gives the bound from the second column of Table A.1 for each of the values of n in the first column, as required.

5. $r = 5$. The possible lists of chief factors of the primitive group R of degree 5 can be obtained from the MAGMA database [6]. In particular, applying (6.3.2) yields

$$d(G) \leq 2E''(s,2) + E''(s,5) + d(S).$$

Again, combining this with the bounds on $d(S)$ described above yields the required bound from Table A.1 in each case.

6. $r = 6$. Again, we take the possible lists of chief factors of the primitive group R of degree 6 from the MAGMA database [6], and apply (6.3.2). We get

$$d(G) \leq E''(s,2) + 1 + d(S).$$

Combining this with the bounds on $d(S)$ described above yields the required bound from Table A.1 in each of the relevant cases.

7. $r = 8$. After obtaining the possible chief factors of R from the MAGMA database, we again apply (6.3.2) and get

$$d(G) \leq 3E''(s,2) + E''(s,3) + E''(s,7) + d(S).$$

Using the above with the bounds on $d(S)$ described previously gives the required bound from Table A.1 in each case.

8. $10 \leq r \leq 16$. In each case, we use the same approach as in the previous case, so to avoid being too repetitive we will just check the $r = 16$ case. Again we can take the possible lists of chief factors of the primitive groups R of degree 16 from the MAGMA database, and apply (6.3.2). We get

$$d(G) \leq 7E''(s,2) + E''(s,3) + \max\{E''(s,3), E''(s,5)\} + d(S).$$

As before, combining this with the usual bounds for $d(S)$ gives the bounds in Table A.1 in each case.

(iii) We now consider the bounds in Table A.2., i.e. the exceptional cases from Theorem 6.1.3. Thus, either $n = 2^m5$ and $17 \leq m \leq 26$, or $n = 2^m15$ and $15 \leq m \leq 35$. Note that $0 \leq \mathrm{bl}_2(G) \leq m$. If $\mathrm{bl}_2(G) = 0$ then (6.3.1) for $r > 16$, and (6.3.2) for $2 < r \leq 16$, as in our proofs in **(i) and (ii)** above yields the required bounds in each case.

So assume that $\mathrm{bl}_2(G) \geq 1$. Then

$$d(G) \leq \sum_{i=1}^{\mathrm{bl}_2(G)} E(2^{m-i}5, 2) + d(\widetilde{S}) \tag{6.3.5}$$

where $\widetilde{S}$ is transitive of degree $2^{m-\mathrm{bl}_2(G)}v$, by Corollary 6.2.7 Part (ii).

Now, fix a transitive permutation group G of degree n where n is one of the values from the first column of Table A.2. Suppose first that $\mathrm{bl}_2(G) \leq f$, where f is the corresponding value to n in the second column of Table A.2. To bound $d(\widetilde{S})$ above, we use Table B.1 (Appendix B) if $2 \leq 2^{m-\mathrm{bl}_2(G)}v \leq 32$; otherwise, we use the previous rows of Tables A.1 and A.2. Combining these bounds for $d(\widetilde{S})$ with (6.3.5) yields $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$ in each case, as required.

If G contains a soluble transitive subgroup, then the bound at (6.3.5) with E replaced by E_{sol} holds, and yields $d(G) \leq \lfloor c_1 n/\sqrt{\log n} \rfloor$ in each case, as needed.

So we may assume that $\mathrm{bl}_2(G) > f$, and that G contains so soluble transitive subgroups. In particular, the bound at (6.3.5) again holds. If $\widetilde{S}$ is primitive of degree $2^{m-\mathrm{bl}_2(G)}v$, then the bound $d(\widetilde{S}) \leq \lfloor \log(2^{m-\mathrm{bl}_2(G)}v) \rfloor$ of Theorem 2.1.15 gives us the required bound in Table A.2 in each case. So assume that $\widetilde{S}$ is imprimitive, with minimal block size $\widetilde{r} > 2$. Also, write $\widetilde{s} := 2^{m-f_G}v/\widetilde{r}$. With (r, s) replaced by $(\widetilde{r}, \widetilde{s})$, we can now apply (6.3.1) if $\widetilde{r} > 16$, and (6.3.2) for $2 < r \leq 16$, as in cases (i) and (ii) above. (Note that $d_{trans}(\widetilde{S})$ is bounded above using Table B.1 if $2 \leq \widetilde{s} \leq 32$). This gives us the required bound in Table A.2 in each case. (We perform these calculations for each possible value of f_G, and each pair $(\widetilde{r}, \widetilde{s})$ with $\widetilde{r} > 2$ and $2^{m-f_G}v = \widetilde{r}\widetilde{s}$.) This completes the proof.

□

We are now ready to prove Theorem 6.1.3.

Proof of Theorem 6.1.3. The proof is by induction on n. Suppose first that G is primitive. The result clearly holds when $n \leq 3$. When $n \geq 4$, we have $\log n \leq c_1 n/\sqrt{\log n}$, so the result follows immediately from Theorem 2.1.15. This can serve as the initial step.

The inductive step concerns imprimitive G. For this, we now use the notation introduced immediately following Theorem 6.2.2. Write V_i for the abelian chief factors of R, and write $|V_i| = p_i^{a_i}$. Recall that $a(R)$ denotes the composition length of R. In particular, $a(R) \geq \sum_i a_i + c_{nonab}(R)$. The inductive hypothesis, together with the bounds obtained in Corollaries 5.4.18 and 2.1.16, give

$$d(G) \leq \left\lfloor \frac{2a(R)s}{c' \log s} \right\rfloor + \left\lfloor \frac{c_1 s}{\sqrt{\log s}} \right\rfloor \qquad \text{(if } 2 \leq s \leq 1260\text{)} \qquad (6.3.6)$$

$$d(G) \leq \left\lfloor \frac{a(R)b\sqrt{2}s}{\sqrt{\log s}} \right\rfloor + \left\lfloor \frac{cs}{\sqrt{\log s}} \right\rfloor \qquad \text{(if } s \geq 1261\text{)} \qquad (6.3.7)$$

$$d(G) \leq \left\lfloor \frac{a(R)\frac{2}{c'}s}{\sqrt{\log s}} \right\rfloor + \left\lfloor \frac{cs}{\sqrt{\log s}} \right\rfloor \qquad \text{(for all } s \geq 2\text{)} \qquad (6.3.8)$$

$$d(G) \leq s\lfloor \log r \rfloor + \left\lfloor \frac{cs}{\sqrt{\log s}} \right\rfloor \qquad \text{(for } r \geq 4,\ s \geq 2\text{)} \qquad (6.3.9)$$

respectively. Note that (6.3.6) and (6.3.7) follow from Corollaries 5.4.18 and 6.2.7 Part (i), and together imply (6.3.8), while (6.3.9) follows from Corollary 2.1.16. Recall that we need to prove that $d(G) \leq c_1 rs/\sqrt{\log rs}$ for all cases apart from those listed in Theorem 6.1.3 Part (2).

Suppose first that $r \geq 481$. Then 6.3.8, together with Theorem 2.1.14, gives

$$d(G) \leq \frac{([(2 + c_0)\log r - (1/3)\log 24]\frac{2}{c'} + c)s}{\sqrt{\log s}}.$$

This is less than $c_1 rs/\sqrt{\log rs}$ for $r \geq 481$ and $s \geq 2$, which gives us what we need.

So we may assume that $2 \leq r \leq 480$. Suppose first that $10 \leq r \leq 480$, and consider the function

$$f(e, z, w) = \frac{(eb\sqrt{2} + c)\sqrt{z + w}}{2^z \sqrt{w}}$$

defined on triples of positive real numbers. Clearly when the pair (e, z) is fixed, f becomes a decreasing function of w. We distinguish two sub-cases:

(a) $s \geq 1261$. For each of the cases $10 \leq r \leq 480$, we compute the maximum value $a_{prim}(r)$ of the composition lengths of the primitive groups of degree r, using MAGMA. Each time, we get $f(a_{prim}(r), \log r, \log s) \leq f(a_{prim}(r), \log r, \log 1261) < c_1$, and the result then follows, in each case, from (6.3.7).

(b) $2 \leq s \leq 1260$. For each fixed r, $10 \leq r \leq 480$, and each s, $2 \leq s \leq 1260$, we explicitly compute $\min\{\lfloor 2a_{prim}(r)s/(c' \log s)\rfloor, s\lfloor \log r \rfloor\} + \lfloor c_1 s/\sqrt{\log s}\rfloor$. Each time, except when $r = 16$ and $72 \leq s \leq 1260$, this integer is less than or equal to $\lfloor c_1 rs/\sqrt{\log rs}\rfloor$, which, after appealing to the inequalities at (6.3.6) and (6.3.9), gives us what we need. If $r = 16$, and $72 \leq s \leq 1260$, we have $d(G) \leq 7E(s,2) + 2E(s,3) + \lfloor c_1 s/\sqrt{\log s}\rfloor$, by Corollary 6.2.7 Part (i), and this gives the required bound in each case (the chief factors of the primitive groups of degree 16 are computed using MAGMA - see Table B.2).

Finally, we deal with the cases $2 \leq r \leq 9$. In considering each of the relevant cases, we take the possible lists of chief factors of R from the MAGMA database. In each case, we bound $d(S)$ above by using Table B.1 if $2 \leq s \leq 32$, Lemma 6.3.1 if s is in the left hand column of Table A.1 or Table A.2, or the inductive hypothesis otherwise.

(a) $r = 2$. Corollary 6.2.7 Part (i) gives $d(G) \leq E(s,2) + d(S)$. Write $s = 2^m q$, where q is odd, and assume first that $s < 10^{66}$. If $\mathrm{lpp}(q) \geq 19$, then $d(G) \leq s/19 + c_1 s/\sqrt{\log s}$, using the inductive hypothesis, and this is less than $2c_1 s/\sqrt{\log 2s}$ for $s < 10^{66}$. So assume further that $\mathrm{lpp}(q) \leq 17$. Then q is of the form $q = 3^{l_3}5^{l_5}7^{l_7}11^{l_{11}}13^{l_{13}}17^{l_{17}}$, where $0 \leq l_3 \leq 2$, and $0 \leq l_i \leq 1$, for $i = 5$, 7, 11, 13 and 17. Fix one such q. Then $0 \leq m \leq m(q) := \lfloor \log(10^{66}/q)\rfloor$, and by using the upper bounds on $d(S)$ described above, we have the upper bound $d(G) \leq E(2^m q, 2) + d(S)$. We repeat this for each of the 96 possible values of q, and each $0 \leq m \leq m(q)$. In each case, the upper bound computed gives us what we need.

Thus, we may assume that $s \geq 10^{66}$. We distinguish two sub-cases.

(i) $s_2 \geq s^{858/1000}$. Then $E(s,2) \leq bs/\sqrt{\log s_2} \leq bs\sqrt{1000/858}/\sqrt{\log s}$. Hence, $d(G) \leq bs\sqrt{1000/858}/\sqrt{\log s} + c_1 s/\sqrt{\log s}$, and this is less than or equal to $2c_1 s/\sqrt{\log 2s}$ for $s \geq 10^{66}$, as required.

(ii) $s/s_2 \geq s^{142/1000}$. Then, by Lemma 2.4.2, we have

$$E(s,2) \leq s/(c' \log(s/s_2)) \leq (1000/142)s/c' \log s,$$

and hence $d(G) \leq (1000/142)s/(c' \log s) + c_1 s/\sqrt{\log s}$. Again, this is less than or equal to $2c_1 s/\sqrt{\log 2s}$, for $s \geq 10^{66}$.

(b) $r = 3$. Here, Corollary 6.2.7 Part (i) gives $d(G) \leq E(s,3) + E(s,2) + d(S)$. Using the bounds for $d(S)$ described above, this gives us what we need whenever $2 \leq s \leq 5577$, and whenever S is one of the exceptional cases listed in Theorem 6.1.3 Part (2))in these cases, we take the bounds for $d(S)$ from Table A.2). Otherwise, $s \geq 5578$, and we use Corollary 5.4.18 to distinguish two cases, with $\alpha = 1/3$.

(i) $s_2,\ s_3 \leq s^{1/3}$. Then $d(G) \leq 3s/(c' \log s) + c_1 s/\sqrt{\log s}$, and this is less than or equal to $3c_1 s/\sqrt{\log 3s}$ for $s \geq 3824$.

(ii) $s_2 \geq s^{1/3}$, or $s_3 \geq s^{1/3}$. Then $\mathrm{lpp}\,(s/s_3) \geq s^{1/3}$ or $\mathrm{lpp}\,(s/s_2) \geq s^{1/3}$, so $d(G) \leq b\sqrt{3}s/\sqrt{\log s} + s^{2/3} + c_1 s/\sqrt{\log s}$, and this is at most $3c_1 s/\sqrt{\log 3s}$, for $s \geq 5578$.

(c) $r = 4$. Here Corollary 6.2.8 implies that

$$d(G) \leq E(s,2) + \min\left\{\frac{bs}{\sqrt{\log s_2}}, \frac{s}{s_3}\right\} + E(s,3) + d(S).$$

Using the bounds on $d(S)$ described above, this yields the required upper bound whenever S is one of the exceptional cases of Theorem 6.1.3 Part (2), and whenever $7 \leq s \leq 115062$. When $2 \leq s \leq 6$, G is transitive of degree $4s$, and the result follows by using Table B.1. So assume that $s \geq 115063$, and that s is not one of those cases listed in Theorem 6.1.3 Part (2). Using Corollary 5.4.18, with $\alpha = 45/100$, we distinguish three cases.

(i) $s_2,\ s_3 \leq s^{45/100}$. Then $d(G) \leq (300/55)s/(c' \log s) + c_1 s/\sqrt{\log s}$, and this is less than or equal to $4c_1 s/\sqrt{\log 4s}$ for $s \geq 115063$, as needed.

(ii) $s_2 \geq s^{45/100}$. Then $d(G) \leq 2\sqrt{100/45}bs/\sqrt{\log s} + s^{55/100} + c_1 s/\sqrt{\log s}$, and this is at most $4c_1 s/\sqrt{\log 4s}$, for $s \geq 82517$.

(iii) $s_3 \geq s^{45/100}$. Then $d(G) \leq \sqrt{100/45}bs/\sqrt{\log s} + 2s^{55/100} + c_1 s/\sqrt{\log s}$, which is less than or equal to $4c_1 s/\sqrt{\log 4s}$, for $s \geq 44$. This completes the proof of the theorem in the case $r = 4$.

(d) $r = 5$. Corollary 6.2.7 Part (i) gives $d(G) \leq E(s,5) + 2E(s,2) + d(S)$. Again, this gives us what we need for each s in the range $3 \leq s \leq 552$, and each exceptional S. Also, $s = 2$ implies that G is transitive of degree 10, and the

result follows from Table B.1. Thus, we may assume that $s \geq 553$. Applying Corollary 5.4.18, with $\alpha = 2/5$, yields three cases.

(i) $s_2,\ s_5 \leq s^{2/5}$. Then $d(G) \leq 5s/(c' \log s) + c_1 s/\sqrt{\log s}$, which is less than or equal to $5c_1 s/\sqrt{\log 5s}$ for $s \geq 553$, as required.

(ii) $s_2 \geq s^{2/5}$. Then $d(G) \leq 2b\sqrt{5/2}s/\sqrt{\log s} + s^{3/5} + c_1 s/\sqrt{\log s}$, and this is no greater than $5c_1 s/\sqrt{\log 5s}$ when $s \geq 139$.

(iii) $s_5 \geq s^{2/5}$. Then $d(G) \leq b\sqrt{5/2}s/\sqrt{\log s} + 2s^{3/5} + c_1 s/\sqrt{\log s}$, which is less than or equal to $5c_1 s/\sqrt{\log 5s}$ for $s \geq 17$.

(e) $r = 6$. Here, Corollary 6.2.7 Part (i), together with the inductive hypothesis, gives $d(G) \leq E(s,2) + 1 + d(S)$. Using the usual bounds on $d(S)$, this is at most $\lfloor 6cs/\sqrt{\log 6s} \rfloor$ for $2 \leq s \leq 1260$, and whenever S is one of the exceptional cases. Otherwise, $s \geq 1261$, and $d(S) \leq c_1 s/\sqrt{\log s}$. Hence, by Corollary 5.4.18 Part (iii), $d(G) \leq b\sqrt{2}s/\sqrt{\log s} + 1 + cs/\sqrt{\log s}$, which is less than or equal to $6c_1 s/\sqrt{\log 6s}$ for $s \geq 2$. This completes the proof of the theorem in the case $r = 6$.

(f) $r = 7$. Here, $d(G) \leq E(s,2)+E(s,3)+E(s,7)+d(S)$, again using Corollary 6.2.7 Part (i). Bounding $d(S)$ as described previously, this is at most $\lfloor 7c_1 s/\sqrt{\log 7s} \rfloor$ for each s in the range $2 \leq s \leq 1260$, and each exceptional S. Otherwise, $s \geq 1261$, and by Corollary 5.4.18 Part (iii) $d(G) \leq 3b\sqrt{2}s/\sqrt{\log s} + c_1 s/\sqrt{\log s}$. This is less than $7c_1 s/\sqrt{\log 7s}$ for $s \geq 7$, and, again, we have what we need.

(g) $r = 8$. Using Corollary 6.2.7 Part (i), $d(G) \leq 3E(s,2)+E(s,3)+E(s,7)+d(S)$. In each of the cases $2 \leq s \leq 272$, and each exceptional case, this bound, together with the bounds on $d(S)$ described above, give us what we need. Thus, we may assume that $s \geq 273$. Then the inductive hypothesis gives $d(S) \leq c_1 s/\sqrt{\log s}$, and applying Corollary 5.4.18, with $\alpha = 37/100$, yields three cases.

(i) $\max\{s_2, s_3, s_7\} \leq s^{37/100}$. Then $d(G) \leq (500/63)s/(c' \log s) + c_1 s/\sqrt{\log s}$, which is less than or equal to $8c_1 s/\sqrt{\log 8s}$ for $s \geq 273$, as required.

(ii) $s_2 \geq s^{37/100}$. Then $d(G) \leq 3b\sqrt{100/37}s/\sqrt{\log s} + 2s^{63/100} + c_1 s/\sqrt{\log s}$, and this is no greater than $8c_1 s/\sqrt{\log 8s}$ when $s \geq 98$.

(iii) $\max\{s_3, s_7\} \geq s^{37/100}$. Then $d(G) \leq 2b\sqrt{100/37}s/\sqrt{\log s} + 3s^{63/100} + c_1 s/\sqrt{\log s}$, which is less than or equal to $8c_1 s/\sqrt{\log 8s}$ for $s \geq 27$.

(h) $r = 9$. By Corollary 6.2.7 Part (i), $d(G) \leq 4E(s,2) + 3E(s,3) + d(S)$. When $3 \leq s \leq 2335$, and when S is one of the exceptional cases, this bound, together with the usual bounds on $d(S)$, give us what we need. If $s = 2$, then G is transitive of degree 18, and the result follows from Table A.1. Otherwise, $s \geq 2336$, and $d(S) \leq c_1 s/\sqrt{\log s}$, using the inductive hypothesis. We now use Corollary 5.4.18 to distinguish three cases, with $\alpha = 37/100$.

(i) $s_2,\ s_3 \leq s^{37/100}$. Then $d(G) \leq (700/63)s/(c' \log s) + c_1 s/\sqrt{\log s}$, and this is less than or equal to $9c_1 s/\sqrt{\log 9s}$ for $s \geq 2336$, as needed.

(ii) $s_2 \geq s^{37/100}$. Then $d(G) \leq 4b\sqrt{100/37}s/\sqrt{\log s} + 3s^{63/100} + c_1 s/\sqrt{\log s}$, which is no larger than $9cs/\sqrt{\log 9s}$, whenever $s \geq 1197$.

(iii) $s_3 \geq s^{37/100}$. Here, $d(G) \leq 3b\sqrt{100/37}s/\sqrt{\log s} + 4s^{63/100} + c_1 s/\sqrt{\log s}$, and this is less than or equal to $9c_1 s/\sqrt{\log 9s}$ for $s \geq 148$.

This completes the proof of Theorem 6.1.3. □

We conclude with the example mentioned in the introduction, which shows that the bound of Theorem 6.1.3 is of the right form. This family of examples is constructed in [28, (3.2)].

Example 6.3.2. Let A be an elementary abelian group of order 2^{2k-1}, and write R for the radical of the group algebra $\mathbb{F}_2[A]$. For a positive integer t, write $R^t := \{a_1 a_2 \dots a_t : a_i \in R\}$, and consider the 2-group $G := R^{k-1} \rtimes A$.

The largest trivial submodule of $\mathbb{F}_2[A]$ is 1-dimensional, while $\dim(R^{k-1}) > 1$, by [28, 3.2]. Hence, the centraliser $C_A(R^{k-1})$ of R^{k-1} in A is a proper characteristic subgroup of A; since A is characteristically simple, it follows that $C_A(R^{k-1}) = 1$. Thus, $C_G(R^{k-1}) = R^{k-1}$, so $Z := Z(G) = C_{R^{k-1}}(A)$. Again, since the largest trivial submodule of $\mathbb{F}_2[A]$ is 1-dimensional, and Z is nontrivial, it follows that Z has order 2, and hence Z is the unique minimal normal subgroup of G. Let H be a subspace complement to Z in R^{k-1}. Then H has codimension 1 in R^{k-1}, and hence has index 2^{2k} in G. It is also clear that H is core-free in G, so G is a transitive permutation group of degree 2^{2k}.

Next, note that

$$\sqrt{2k}\binom{2k}{k}\frac{1}{4^k} = \left[\frac{1}{2}\left(\frac{3}{2}\frac{3}{4}\right)\left(\frac{5}{4}\frac{5}{6}\right)\cdots\left(\frac{2k-1}{2k-2}\frac{2k-1}{2k}\right)\right]^{1/2} = \left[\frac{1}{2}\prod_{j=2}^{k}\left(1+\frac{1}{4j(j-1)}\right)\right]^{1/2}$$

As in the proof of Corollary 5.2.3, the expression in the middle converges to $b = \sqrt{2/\pi}$, by Wallis' formula. Hence, since the expression on the right is increasing, we conclude that for all $\epsilon > 0$, there exists a positive integer k such that $\sqrt{2k}\binom{2k}{k}\frac{1}{4^k} \geq b - \epsilon$, that is, $\binom{2k}{k} \geq (b-\epsilon)4^k/\sqrt{2k}$.

Now, the derived subgroup G' of G is R^k, and $G/G' \cong (R^{k-1}/R^k) \times A$ is elementary abelian of rank $\binom{2k-1}{k-1} + 2k - 1$, using [28, Proof of (2.4)]. Since G is a 2-group, it follows that $G' = \Phi(G)$. Thus, for large enough k we have

$$d(G) = \binom{2k-1}{k-1} + 2k - 1 = \frac{1}{2}\binom{2k}{k} + 2k - 1 \geq \frac{(b-\epsilon)2^{2k}}{2\sqrt{2k}} + 2k - 1.$$

Chapter 7

Enumerating subgroups of $\mathrm{Sym}(n)$: A reduction of a conjecture of Pyber

7.1 Introduction

Apart from its independent interest, the invariant $d(G)$ is also useful in subgroup enumeration. Indeed, if G is a finite group and $d(H) \leq m$ for all subgroups H of G, then G has at most $|G|^m$ subgroups. This is often a crude upper bound, but the method can sometimes be used effectively if combined with other results. For instance, every permutation group G of degree n can be generated by a soluble subgroup, together with another element $g \in G$ (see [3]). Moreover

(1) There are at most 2^{17n} maximal soluble subgroups in $\mathrm{Sym}(n)$ [45, Lemma 4.1];

(2) The order of a soluble subgroup of $\mathrm{Sym}(n)$ is at most $24^{\frac{n-1}{3}}$ [21, Theorem 3];

(3) Each subgroup of $\mathrm{Sym}(n)$ can be generated by $\frac{n+1}{2}$ elements [40, Lemma 5.2].

From these results, we deduce that there are at most $2^{17n}24^{\frac{n-1}{3}\frac{n+1}{2}}$ soluble subgroups of $\mathrm{Sym}(n)$, and hence at most $2^{17n}24^{\frac{n-1}{3}\frac{n+1}{2}} \times n! = 24^{o(n^2)+\frac{n^2}{6}}$ subgroups of $\mathrm{Sym}(n)$ in total. This proof is due to Pyber [45, Theorem 4.2], and his result in full reads as follows.

Theorem 7.1.1. *Let* $\mathrm{Sub}(\mathrm{Sym}(n))$ *denote the set of subgroups of* $\mathrm{Sym}(n)$. *Then*

$$2^{o(n^2)+\frac{n^2}{16}} \leq |\,\mathrm{Sub}(\mathrm{Sym}(n))| \leq 24^{o(n^2)+\frac{n^2}{6}}.$$

An easy counting argument shows that the elementary abelian subgroup $H := \langle (1,2),(3,4),\ldots\rangle \leq \mathrm{Sym}(n)$, of order $2^{\lfloor \frac{n}{2} \rfloor}$, has $2^{o(n^2)+\frac{n^2}{16}}$ subgroups. Thus, the lower bound in Theorem 7.1.1 is sharp. Furthermore, Pyber conjectures that this is the "correct" bound [44, Page 210]. That is, that *the number of subgroups of* $\mathrm{Sym}(n)$ *is precisely* $2^{o(n^2)+\frac{n^2}{16}}$. For more information see his paper [44], or his excellent survey [45].

In this chapter, we prove a result which reduces Pyber's conjecture. First, we note the following definition.

Definition 7.1.2. Let G be a finite group.

(a) Define $\mathrm{Sub}(G)$ to be set of subgroups of G.

(b) For a positive integer m, define

$$\mathrm{Sub}_m(\mathrm{Sym}(n)) := \{H \leq \mathrm{Sym}(n) : \text{Each } H\text{-orbit has length at most } m\}.$$

Now, J.C. Schlage-Puchta (private correspondence), has proved that if the quantity

$$f(n) := \max\{d(G)\log|G|/n^2 : G \leq \mathrm{Sym}(n) \text{ transitive}\}$$

approaches 0 as n tends to ∞, then there exists an absolute constant $\overline{c}$ such that the number of subgroups of $\mathrm{Sym}(n)$ is at most $2^{o(n^2)}|\mathrm{Sub}_{\overline{c}}(\mathrm{Sym}(n))|$. This reduces Pyber's conjecture to counting the number of subgroups of $\mathrm{Sym}(n)$ which have all orbit lengths bounded above by $\overline{c}$.

Motivated by this, we prove the following result, which was already discussed in Chapter 1.

Theorem 1.2.3. *There exists an absolute constant C such that*

$$d(G) \leq \left\lfloor \frac{Cn^2}{\log|G|\sqrt{\log n}} \right\rfloor$$

whenever G is a transitive permutation group of degree $n \geq 2$.

In particular, the discussed reduction of Pyber's conjecture follows. We remark that the bound in Theorem 1.2.3 is 'asymptotically best possible'. See Example 7.3.3 for more details. We think one could come up with a good estimate for C by using our methods and working a little bit harder on the "small cases", as we did in the proof of Theorem 6.1.3, but we did not do so here.

Our strategy for the proof of Theorem 1.2.3 will be to bound $d(G)\log|G|$, for a fixed transitive group G, in terms of the degrees of a tuple of primitive components for G. The key result in this direction is Proposition 7.3.2, which we prove in Section 6.3. The proof of Theorem 1.2.3 is also contained in Section 6.3, while Section 6.2 contains results on minimal generator numbers, composition length, and orders of transitive groups.

7.2 Preliminary results

7.2.1 Minimal generator numbers in wreath products

In proving Theorem 1.2.3, we will omit reference to the constant C, and just use the Vinogradov notation defined immediately after Definition 5.5.1. We will now restate some results from Chapters 2, 3 and 4 in this language for the convenience of the reader.

We begin with Theorems 2.1.14 and 1.2.2.

Theorem 7.2.1. *Let R be a primitive permutation group of degree r. Then $a(R) \ll \log r$.*

Theorem 7.2.2. *Let S be a transitive permutation group of degree $s \geq 2$. Then $d(S) \ll s/\sqrt{\log s}$.*

We also note the following useful consequence of Corollaries 6.2.6 and 5.4.18, and Theorem 7.2.2.

Corollary 7.2.3. *Let R be a finite group, let S be a transitive permutation group of degree $s \geq 2$, and let G be a large subgroup of the wreath product $R \wr S$. Then*

$$d(G) \ll \frac{a(R)s}{\sqrt{\log s}}.$$

Theorem 2.1.15 reads as follows in Vinogradov notation.

Theorem 7.2.4 (**[25], Theorem 1.1**). *Let H be a subnormal subgroup of a primitive permutation group of degree r. Then $d(H) \ll \log r$.*

Finally, we will need the following theorem of Cameron, Solomon and Turull; note that we only give a simplified version of their result here.

Theorem 7.2.5 (**[10], Theorem 1**). *Let G be a permutation group of degree $n \geq 2$. Then $a(G) \ll n$.*

7.2.2 Orders of transitive permutation groups

We now turn to bounds on the order of a transitive permutation group G, of degree n. First, we fix some notation which will be retained for the remainder of the chapter. Let G be a transitive permutation group of degree n, and let $(R_1, \ldots, R_t)$ be a tuple of primitive components for G, where each R_i is primitive of degree r_i, and $\prod_i r_i = n$. Furthermore, we will write π_1 for the identity map $G \to G$, and for $i \geq 2$, we will write π_i to denote the projection $\pi_i : G\pi_{i-1} \leq R_{i-1} \wr (R_i \wr R_{i+1} \wr \ldots \wr R_t) \to R_i \wr R_{i+1} \wr \ldots \wr R_t$.

The following is a simplified version of a theorem of C. Praeger and J. Saxl [43] (which was later improved by A. Maróti in [39]).

Theorem 7.2.6 (**[43], Main Theorem**). *Let G be a primitive permutation group of degree r, not containing* $\mathrm{Alt}(r)$. *Then* $\log|G| \ll r$.

Since the symmetric and alternating groups are 2-generated, the next corollary follows immediately from Theorems 7.2.4 and 7.2.6.

Corollary 7.2.7. *Let G be a subnormal subgroup of a primitive permutation group of degree r. Then $d(G)\log|G| \ll r\log r$.*

7.3 The proof of Theorem 1.2.3

Before proceeding to the proof of Theorem 1.2.3, we require an application of the results in Section 6.2. First, we need a preliminary lemma.

Lemma 7.3.1. *Let R and S be transitive permutation groups of degree $r \geq 2$ and $s \geq 1$ respectively, let D be a subgroup of* $\mathrm{Sym}(d)$ *containing* $\mathrm{Alt}(d)$, *let P be a large subgroup of the wreath product $D \wr S$, and let G be a large subgroup of $R \wr P$. Also, write U_i for the abelian chief factors of R. Suppose that $d \geq 5$. Then*

(i) There exists a large subgroup Q of the wreath product $R \wr D$, and an embedding $\theta : G \to Q \wr S$, such that $G\theta$ is a large subgroup of $Q \wr S$.

(ii) Let $H := N_Q(R_{(1)})$. Then Q has a normal series

$$1 = N_0 \leq N_1 \leq \ldots < N_t < N_{t+1} \leq N_{t+2} = Q,$$

where for each abelian U_i with $i \leq t$, N_i/N_{i-1} is contained in the Q-module $U_i \uparrow_H^Q$; and for each non-abelian U_i with $i \leq t$, N_i/N_{i-1} is either trivial or a non-abelian chief factor of Q. Also, $N_{t+1}/N_t \cong \mathrm{Alt}(d)$, and $|N_{t+2}/N_{t+1}| \leq 2$.

Proof. Note first that G is an imprimitive permutation group of degree rds, with a block Δ_1 of size r, by Remark 2.1.8. Now, by Remark 2.1.11, G is also a subgroup of the wreath product $X := (R \wr D) \wr S$. Hence, G also has a block of size rd, again using Remark 2.1.8. Let Δ be a block of size rd containing Δ_1. Let $H_1 := \mathrm{Stab}_G(\Delta_1)$ and $H := \mathrm{Stab}_G(\Delta)$. Then $H_1 \leq H$, and Δ_1 is a block for H^Δ of size r, with block stabiliser H_1^Δ. Let Γ_1 be the set of H-translates of Δ_1, and let Γ be the set of G-translates of Δ. Then G is a large subgroup of $H^\Delta \wr G^\Gamma$, while H^Δ is a large subgroup of $H_1^{\Delta_1} \wr H^{\Gamma_1}$, by Theorem 2.1.9. By Definition 2.1.7, $H_1^{\Delta_1} \cong R$. Thus, to complete the proof of Part (i) we just need to show that $H^{\Gamma_1} \cong D$ and $G^\Gamma \cong S$ (we then take $Q = H^\Delta$).

First, let $\pi : G \leq R \wr P \to P$ denote projection over the top group. Note that $H\pi \leq P$ is a permutation group of degree ds, stabilising a block of size d. Furthermore, since $\mathrm{Ker}(\pi) = \mathrm{core}_G(H_1) \leq H_1 \leq H$, we have $s = |G : H| = |G\pi : H\pi|$. Thus, $H\pi$ is the full (set-wise) stabiliser of a block for P of size d. It follows that $H^{\Gamma_1} \cong D$, since P is large in $D \wr S$.

Since $\mathrm{Ker}(\pi) = \mathrm{Ker}_G(\Delta_1^G) \leq \mathrm{Ker}_G(\Gamma)$, we have $G^\Gamma \cong \pi(G)^\Gamma = P^\Gamma = S$, as needed. Finally, since Q is a large subgroup of $R \wr D$, and $D \cong \mathrm{Alt}(d)$ or $D \cong \mathrm{Sym}(d)$, Part (ii) follows from Lemma 6.2.5. □

The mentioned application can now be given as follows.

Proposition 7.3.2. *Let R be a finite group, let S be a transitive permutation group of degree $s \geq 2$, let D be a subgroup of* $\mathrm{Sym}(d)$ *containing* $\mathrm{Alt}(d)$*, let P be a large subgroup of the wreath product $D \wr S$, and let G be a large subgroup of $R \wr P$. Also, let K_1 be the kernel of the action of $P \leq D \wr S$ on a set of blocks of size d, and let A be the induced action of K_1 on a fixed block Δ for P. Assume that $A \neq 1$, that $d \geq 5$, and set $g(d, s) := \max\{1, \frac{d}{\sqrt{\log s}}\}$. Then*

(i) $d(G) \ll a(R)s$*; and*

(ii) $d(G) \ll \frac{a(R)g(d,s)s}{\sqrt{\log s}}$.

Proof. Let U_i, for $1 \leq i \leq t$ say, denote the chief factors of R. Also, if U_i is abelian, write $|U_i| = p_i^{a_i}$, for p_i prime. By Lemma 7.3.1 Part (i), G is a large subgroup of $Q \wr S$, where Q is a large subgroup of $R \wr D$. Let $H_1 := N_Q(R_{(1)})$. By Lemma 7.3.1 Part (ii), Q has a normal series

$$1 = N_0 \leq N_1 \leq \ldots \leq N_t < N_{t+1} \leq N_{t+2} = Q,$$

where each abelian factor N_i/N_{i-1}, for $i \leq t$, is contained in the Q-module $U_i \uparrow_{H_1}^{Q}$, and each nonabelian factor is a chief factor of Q. Also, $N_{t+1}/N_t \cong \mathrm{Alt}(d)$, and $|N_{t+2}/N_{t+1}| \leq 2$. In particular,

$$c_{nonab}(Q) \leq c_{nonab}(R) + 1. \tag{7.3.1}$$

Denote by B the base group of $Q \wr S$, and consider the corresponding normal series

$$1 = G \cap B_{N_0} \leq G \cap B_{N_1} \leq G \cap B_{N_2} \leq \ldots \leq G \cap B_{N_t} \tag{7.3.2}$$

$$< G \cap B_{N_{t+1}} \leq G \cap B_{N_{t+2}} = G \cap B \tag{7.3.3}$$

for $G \cap B$. Let M_i be the abelian factors in (7.3.2). Then

$$d(G) \ll \sum_{U_i \text{ abelian}} d_G(M_i) + c_{nonab}(R) + \frac{s}{\sqrt{\log s}} \tag{7.3.4}$$

by Corollary 6.2.6 and Theorem 7.2.2. Viewing G as a subgroup of $Q \wr S$, let $H := N_G(Q_{(1)})$. Also, let $\pi : R \wr P \to P$ denote projection over the top group. Since $H\pi \leq P$ stabilises a block of size d, we may assume, without loss of generality, that

$$H\pi = \mathrm{Stab}_P(\Delta)$$

(recall that Δ is a block of size d for $P \leq D \wr S$). Note also that M_i is a submodule of the induced module $U_i \uparrow_{H_1}^{H} \uparrow_{H}^{G} \cong U_i \uparrow_{H_1}^{G}$, by Lemmas 6.2.5 and 7.3.1.

Fix i in the range $1 \leq i \leq t$ such that U_i is abelian. Suppose first that $s_{p_i} \leq \sqrt{s}$. Then Corollary 5.4.18 Part (ii), with $\alpha := 1/2$, gives

$$d_G(M_i) \ll \frac{a_i d s}{\log s} \leq \frac{a_i g(d,s) s}{\sqrt{\log s}} \tag{7.3.5}$$

Assume next that $s_{p_i} > \sqrt{s}$ for some fixed i. Let $K := \mathrm{core}_G(H)$. Note that $K\pi = K_1 \leq P$, since $H\pi = \mathrm{Stab}_P(\Delta)$ is a block stabiliser. Then

$$1 < A = (K\pi)^{\Delta} \trianglelefteq (H\pi)^{\Delta} = D,$$

so $(K\pi)^{\Delta} \geq \mathrm{Alt}(d)$. Hence, Proposition 5.5.2 Part (ii) implies that

$$d_G(M_i) \ll \frac{a_i s}{\sqrt{\log s_{p_i}}} \leq \frac{\sqrt{2} a_i s}{\sqrt{\log s}} \ll \frac{a_i g(d,s) s}{\sqrt{\log s}}. \tag{7.3.6}$$

Thus, (7.3.4), (7.3.5) and (7.3.6) yield:

$$\begin{aligned} d(G) &\ll \sum_{U_i \text{ abelian}} \frac{a_i g(d,s)s}{\sqrt{\log s}} + c_{nonab}(R) + \frac{s}{\sqrt{\log s}} \\ &\ll \frac{a(R)g(d,s)s}{\sqrt{\log s}} + \frac{s}{\sqrt{\log s}} \\ &\ll \frac{a(R)g(d,s)s}{\sqrt{\log s}} + \frac{g(d,s)s}{\sqrt{\log s}} \ll \frac{a(R)g(d,s)s}{\sqrt{\log s}} \end{aligned}$$

and this proves Part (ii).

Finally, 7.3.4 and Proposition 5.5.2 Part (i) give

$$\begin{aligned} d(G) &\ll \sum_{U_i \text{ abelian}} a_i s + c_{nonab}(R) + \frac{s}{\sqrt{\log s}} \\ &\ll a(R)s + \frac{s}{\sqrt{\log s}} \ll a(R)s \end{aligned}$$

and this completes the proof. □

We are now ready to prove Theorem 1.2.3.

Proof of Theorem 1.2.3. Let $f(G) = d(G)\log|G|\sqrt{\log n}/n^2$. We will prove, by induction on n, that $f(G) \ll 1$. If G is primitive, then $f(G) \ll (\log n)^{3/2}/n$ by Corollary 7.2.7, and the claim follows.

For the inductive step, assume that G is imprimitive. Fix a tuple $(R_1, R_2, \ldots, R_t)$ of primitive components for G, where each R_i is primitive of degree r_i, say. Also, for $1 \leq i \leq t-1$, let Δ_i be a block of size r_i for $\pi_i(G) \leq R_i \wr \pi_{i+1}(R_i)$, and denote by A_i the induced action of $\mathrm{Ker}_{\pi_i(G)}(\{{\Delta_i}^g : g \in \pi_i(G)\})$ on Δ_i (in particular, note that $A_i \trianglelefteq R_i$). Finally, set $A_t := \pi_t(G)$. Then

$$|G| \leq \prod_{i=1}^{t} |A_i|^{\frac{n}{r_1 \cdots r_i}} \tag{7.3.7}$$

Next, for $1 \leq i \leq t$, we define the functions f_i as follows

$$f_i(G) := \frac{d(G)n\log|A_i|\sqrt{\log n}}{r_1 r_2 \ldots r_i n^2} = \frac{d(G)\log|A_i|\sqrt{\log n}}{r_1 r_2 \ldots r_i n} \tag{7.3.8}$$

The inequality at 7.3.7 then yields $f(G) \leq \sum_{i=1}^{t} f_i(G)$. We claim that $f_i(G) \ll \frac{(i-1)}{2^{i-1}}$ for $2 \leq i \leq t$, and that $f_1(G) \ll 1$. The result will then follow. Indeed, in this case, $f(G) \ll \sum_{i=1}^{\infty} \frac{i-1}{2^{i-1}} \ll 1$.

To this end, first fix i in the range $2 \leq i \leq t$. Clearly we may assume that A_i is non-trivial. Let $D = R_i$, $S := \pi_i(G)$, and note that G is a large subgroup of a wreath product $R \wr P$, where R is transitive of degree $r := r_1 r_2 \dots r_{i-1}$, and P is a large subgroup of $D \wr S$. Set $d := r_i$, $s := r_{i+1} \dots r_t$, and $m := \max\{r, d, s\}$. Suppose first that $d \geq 5$ and that D contains the alternating group $\mathrm{Alt}(d)$. (In particular, we are in the "bottom heavy" situation of Proposition 7.3.2.) Then A_i, being a nontrivial normal subgroup of D, also contains $\mathrm{Alt}(d)$. Note that $|A_i| \leq d^d$. We distinguish two cases. Note throughout that $\log n \leq \log m^3 \ll \log m$.

1. $s \leq 2^{(\log d)^2}$. Then $n = rds \leq m_1^2 2^{(\log m_1)^2}$, where $m_1 := \max\{r, d\}$. Thus, $\log n \leq 2 \log m_1 + (\log m_1)^2 \ll (\log m_1)^2$. Since $a(R) \ll r$ by Theorem 7.2.5, Proposition 7.3.2 Part (i) then implies that $d(G) \ll rs$. Hence, from 7.3.8 we deduce

$$f_i(G) \ll \frac{rsd \log d \log m_1}{r^2 d^2 s} = \frac{\log d \log m_1}{rd} \ll \frac{\log r}{r} \leq \frac{(i-1)}{2^{i-1}}$$

   since $r \geq 2^{i-1}$, and this gives us what we need.

2. $s > 2^{(\log d)^2}$. Note that $m \in \{r, s\}$ in this case. Set $g(d, s) := \max\left\{1, \frac{d}{\sqrt{\log s}}\right\}$. Then

$$g(d, s) \log d \leq d \tag{7.3.9}$$

   since $\sqrt{\log s} > \log d$. Now, Theorem 7.2.5 gives $a(R) \ll r$. Hence, Proposition 7.3.2 Part (ii) gives $d(G) \ll \frac{rg(d,s)s}{\sqrt{\log s}}$. Hence, since $n \leq m^3$, we have

$$\begin{aligned} f_i(G) &\ll \frac{rg(d,s)sd \log d \sqrt{\log m}}{r^2 d^2 s \sqrt{\log s}} \\ &= \frac{g(d,s) \log d \sqrt{\log m}}{rd\sqrt{\log s}} \\ &\leq \frac{d\sqrt{\log m}}{rd\sqrt{\log s}} && \text{by (7.3.9)}, \\ &\leq \frac{\sqrt{\log r}}{r} \leq \frac{\sqrt{i-1}}{2^{i-1}} && \text{since } m \in \{r, s\}. \end{aligned}$$

   This gives us what we need.

Next, suppose that either $d \leq 4$, or that D does not contain $\mathrm{Alt}(d)$. Then $\log |A_i| \ll d$ by Theorem 7.2.6. Now, G is a large subgroup of $R \wr P$, where P is

transitive of degree ds. Also, $a(R) \ll r$ by Theorem 7.2.5. Then, by Corollary 7.2.3 we have

$$d(G) \ll \frac{rds}{\sqrt{\log ds}}.$$

Thus

$$f_i(G) \ll \frac{rdsd\sqrt{\log m}}{r^2d^2s\sqrt{\log ds}} = \frac{\sqrt{\log m}}{r\sqrt{\log ds}} \leq \frac{\sqrt{\log r}}{r} \leq \frac{\sqrt{i-1}}{2^{i-1}}$$

and again this gives us what we need.

Finally, we deal with the case $i = 1$. Here, set $r := r_1$, $s := r_2r_3 \dots r_t$, and $m = \max\{r, s\}$. Then $|A_i| \leq r^r$ and $\log n \ll \log m$. Also, G is a large subgroup of a wreath product $R \wr S$, where R is primitive of degree r, and S is transitive of degree s. Thus, $a(R) \ll \log r$ by Theorem 7.2.1. Thus, Corollary 7.2.3 implies that $d(G) \leq s \log r/\sqrt{\log s}$, and hence

$$f_i(G) \ll \frac{(\log r)sr \log r\sqrt{\log m}}{r^2s\sqrt{\log s}} = \frac{(\log r)^2\sqrt{\log m}}{r\sqrt{\log s}} \leq \frac{(\log r)^{5/2}}{r} \ll 1.$$

This completes the proof. □

We conclude with an example which shows that the bound of Theorem 1.2.3 is asymptotically best possible.

Example 7.3.3. Let A be an elementary abelian group of order 2^{2k-1}, let R be the radical of the group algebra $\mathbb{F}_2[A]$, and let $G := R^{k-1} \rtimes A$ be the 2-group defined in Example 6.3.2, so that G is a transitive permutation group of degree $n := 2^{2k}$. Let $\epsilon > 0$, and recall that for large enough k we have

$$d(G) = \binom{2k-1}{k-1} + 2k - 1 = \frac{1}{2}\binom{2k}{k} + 2k - 1 \geq \frac{(b-\epsilon)2^{2k}}{2\sqrt{2k}} + 2k - 1.$$

Furthermore, $|R^{k-1}| = 2^{\sum_{i=k-1}^{2k-1}\binom{2k-1}{i}} = 2^{2^{2k-1}-2^{k-2}} \sim 2^{n/2}$. Hence, $|G| \sim 2^{n-1}$, which shows that $d(G)\log|G|$ is at least a constant times $n^2/\sqrt{\log n}$.

Appendices

Appendix A

Upper bounds for $d(G)$ for some transitive groups of small degree

We begin with a definition.

Definition A.0.1. Let n be a positive integer. We define

$$d_{trans}(n) := \max\{d(G) : G \text{ is a transitive permutation group of degree } n\}$$

In Table A.2 below, the groups G in the third column are transitive permutation groups of degree n with $\mathrm{bl}_2(G) \geq f$ (see Definition 6.1.1). The upper bounds presented in Table A.2 are proved in Lemma 6.3.1 and Theorem 6.1.3.

Table A.1	
n	$d_{trans}(n) \leq$
48	16
64	20
96	31
128	40
192	57
256	75
384	109
512	145
$2^8 3$	203
2^{10}	271
$2^9 3$	392
2^{11}	523
$2^{10} 3$	738

Table A.1 ctd	
n	$d_{trans}(n) \leq$
$2^{11} 3$	1431
$2^{12} 3$	2718
$2^{13} 3$	5292
$2^{14} 3$	10118
$2^{15} 3$	19770
$2^{16} 3$	38002
$2^{17} 3$	74467
$2^{18} 3$	143750
$2^{19} 3$	282317
$2^{20} 3$	546854
$2^3 5$	9
$2^4 5$	18
$2^5 5$	34

Table A.1 ctd	
n	$d_{trans}(n) \leq$
$2^6 5$	66
$2^7 5$	130
$2^8 5$	258
$2^9 5$	514
$2^{10} 5$	1026
$2^{11} 5$	2050
$2^{12} 5$	4098
$2^{13} 5$	8194
$2^{14} 5$	16386
$2^{15} 5$	32770
$2^{16} 5$	65538
$2^2 15$	15

Table A.1 ctd	
n	$d_{trans}(n) \leq$
$2^3 15$	27
$2^4 15$	52
$2^5 15$	100
$2^6 15$	196
$2^7 15$	388
$2^8 15$	772
$2^9 15$	1540
$2^{10} 15$	3076
$2^{11} 15$	6148
$2^{12} 15$	12292
$2^{13} 15$	24580
$2^{14} 15$	49156

Table A.2		
n	f	$d(G) \leq$
$2^{17}5$	5	130900
$2^{18}5$	4	257722
$2^{19}5$	4	504220
$2^{20}5$	4	984067
$2^{21}5$	4	1919461
$2^{22}5$	4	3745164
$2^{23}5$	5	7312620
$2^{24}5$	5	14290701
$2^{25}5$	6	27953017
$2^{26}5$	7	54725580
$2^{15}15$	6	98308

Table A.2 ctd		
n	f	$d(G) \leq$
$2^{16}15$	4	196612
$2^{17}15$	3	392700
$2^{18}15$	3	773166
$2^{19}15$	3	1512660
$2^{20}15$	3	2952202
$2^{21}15$	3	5758386
$2^{22}15$	3	11235497
$2^{23}15$	3	21937865
$2^{24}15$	3	42872110
$2^{25}15$	3	83859059

Table A.2 ctd		
n	f	$d(G) \leq$
$2^{26}15$	4	164176748
$2^{27}15$	4	321692696
$2^{28}15$	4	630835627
$2^{29}15$	4	1237980292
$2^{30}15$	5	2431149936
$2^{31}15$	5	4777379825
$2^{32}15$	5	9393534359
$2^{33}15$	6	18480443646
$2^{34}15$	7	36376783048
$2^{35}15$	8	71639170628

Remark A.0.2. The bounds in Tables A.1 and A.2 were proved using the methods developed in this thesis (see the proofs of Lemma 6.3.1 and Theorem 6.1.3). We do not expect that they are sharp.

Appendix B

Generator numbers for some transitive groups of small degree

Below is the table of values of $d_{trans}(n)$ for $n \leq 32$. We use the classification of the transitive groups of degree up to 32 [11; 26] and MAGMA [6] to compute these values. The third column of the table contains the numbers i such that

$$d_{trans}(n) = d(\text{TransitiveGroup}(n, i))$$

in the MAGMA database (these numbers are only included when $d_{trans}(n)$ is greater than 2).

Let G be a transitive permutation group of degree $n \leq 32$. Then G is in the MAGMA database, and we use the following procedure to compute $d(G)$.

1. Check if G is cyclic. If so, then $d(G) = 1$ and we are done.

2. Assume that G is not cyclic. If G is a p-group, for some prime p, then we compute the minimal number of generators for the elementary abelian group $G/\Phi(G)$, and this is precisely $d(G)$.

3. Suppose that G is not a p-group. Then we compute all elementary abelian quotients of G. Let m be the largest integer such that G has an elementary abelian quotient of order p^m, for p prime. Then we try to find a generating set for G of size m. If we succeed, then $d(G) = m$, and again we are done.

4. Finally, if none of the previous steps work, we compute $m := d(G/[G,G])$ (which is instantly done since $G/[G,G]$ is abelian), and we try to find a generating set for G of size m. If we succeed, then $d(G) = m$.

The above procedure is of course not guaranteed to compute $d(G)$ exactly for any finite group G, but for each transitive group of degree at most 32 in the MAGMA database, it does work, and so gives us the numbers in Table B.1.

Table B.1		
d	$d_{trans}(n)$	Numbers i such that the max. of $d(G)$ is attained at the group $TransitiveGroup(n,i)$ in the MAGMA database
2	1	
3	2	
4	2	
5	2	
6	2	
7	2	
8	4	[22]
9	3	[5,12,21]
10	3	[27]
11	2	
12	4	[242]
13	2	
14	2	
15	2	
16	6	[197,448,1082,1083,1084,1547]
17	2	
18	4	[89,333,379,380,471,554]
19	2	
20	5	[581,893]
21	3	[64,65,82,95,97,106]
22	2	
23	2	
24	6	[12495,21182,22267,23285,23531,23532,23650,24304]
25	3	[5,9,22,30,33,61,62,70,84,97,109,112]
26	3	[25,43,46,60]
27	6	[894]
28	4	[629,931,936,1153,1158,1300,1305,1448,1832]
29	2	
30	4	[372,636,816,1258,1589,1724,2141,2551,2642,2708,2929,3004, 3305,3429,3430,3437,3462,3483,3490,3844,3871,3872,3873,3874, 3891,4068,4166,4175,4179,4180,4183,4190,4191,4192,4200,4240, 4255,4348,4436,4659,4662,4667,4923,5043,5258,5320]
31	2	
32	10	[1422821,1422822,1514676,2224558,2424619]

Bibliography

[1] Alperin, J.L. *Local Representation Theory.* Cambridge University Press, Cambridge, 1986.

[2] Anderson, I. On primitive sequences. *J. London Math. Soc.* **42** (1967) 137–148.

[3] Aschbacher, M.; Guralnick, R.M. Solvable generation of groups and Sylow subgroups of the lower central series. *J. Algebra* **77** (1982) 189–201.

[4] Babai, L.; Sós, V.T. Sidon sets in groups and induced subgraphs of Cayley graphs. *European J. Combin.* **6(2)** (1985) 101–114.

[5] Benson, D.J. *Representations and Cohomology: Volume 1, Basic Representation Theory of Finite Groups and Associative Algebras.* Cambridge University Press, Cambridge, 1998.

[6] Bosma, W.; Cannon, J.; Playoust, C. The Magma algebra system. I. The user language. *J. Symbolic Comput.* **24** (1997) 235–265.

[7] Bray, J. N.; Holt, D. F.; Roney-Dougal, C. M. *The maximal subgroups of the low-dimensional finite classical groups.* London Math. Soc., Lecture Note Series 407, Cambridge, 2013.

[8] Bryant, R.M.; Kovács, L.G.; Robinson, G.R. Transitive permutation groups and irreducible linear groups. *Quart J. Math.* **46** (1995) 385–407.

[9] Cameron, P.J. *Permutation Groups*, London Math. Soc. (Student Texts), vol. 45, CUP, Cambridge, 1999.

[10] Cameron, P.J.; Solomon, R.G.; Turull, A. Chains of subgroups in symmetric groups. *J. Algebra* **127** (1989) 340–352.

[11] Cannon, J.J.; Holt, D.F. The transitive permutation groups of degree up to 32. *Experimental Math.* **17** (2008) 307–314.

[12] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A. *An ATLAS of Finite Groups.* Clarendon Press, Oxford, 1985; reprinted with corrections 2003.

[13] Curtis, C.W.; Reiner, I. *Representation Theory of Finite Groups and Associative Algebras: Volume I*, Wiley, New York, 1988.

[14] Dalla Volta, F.; Lucchini, A. Finite groups that need more generators than any proper quotient. *J. Austral. Math. Soc.* (Series A) **64** (1998) 82–91.

[15] Dalla Volta, F.; Siemons, J. On solvable minimally transitive permutation groups. *Des. Codes Cryptogr.* **44** (2007) 143–150.

[16] de Bruijn, N.G.; van Ebbenhorst Tengbergen, Ca.; Kruyswijk, D. On the set of divisors of a number. *Nieuw Arch. Wiskunde* **23** (1951) 191–193.

[17] Detomi, E.; Lucchini, A. Probabilistic generation of finite groups with a unique minimal normal subgroup. *J. London Math. Soc.* **87(3)** (2013) 689–706.

[18] Detomi, E.; Lucchini, A. Invariable generation of permutation groups. *Arch. Math.* **104** (2015) 301–309.

[19] Dickson, L.E. *Linear groups: With an exposition of the Galois field theory.* Dover Publications Inc., New York, 1958.

[20] Dilworth, R.P. A decomposition theorem for partially ordered sets. *Ann. of Math.* **51(2)** (1950) 161–166.

[21] Dixon, J.D. The Fitting subgroup of a linear solvable group. *J. Austral. Math. Soc.* **7** (1967) 417–424.

[22] Doerk, K.; Hawkes, T. *Finite soluble groups.* de Gruyter, Berlin, 1992.

[23] Erdös, P. On a Theorem of Sylvester and Schur. *J. London Math. Soc.* **9** (1934) 282–288.

[24] Gorenstein, D. *Finite Groups.* Harper and Row, New York, 1968.

[25] Holt, D.F.; Roney-Dougal, C.M. Minimal and random generation of permutation and matrix groups. *J. Algebra* **387** (2013) 195–223.

[26] Hulpke, A. The minimally transitive groups of degree up to 30. Available at www.math.colostate.edu/ hulpke/paper/ctglist.pdf (electronic).

[27] Isaacs, I.M. *Character Theory of Finite Groups*. Dover, New York, 1994.

[28] Kovács, L.G.; Newman, M.F. Generating transitive permutation groups. *Quart. J. Math. Oxford* (2) **39** (1988) 361–372.

[29] Kleidman, P.; Liebeck, M.W. *The subgroup structure of the finite classical groups*. London Math. Soc., Lecture Note Series 129, Cambridge, 1990.

[30] Liebeck, M. W.; Praeger, C. E.; Saxl, J. Transitive subgroups of primitive permutation groups. *J. Algebra* **234** (2000) 291–361.

[31] Liebeck, M.W; Pyber, L.; Shalev, A. On a conjecture of G.E. Wall. *J. Algebra* **317** (2007) 184–197.

[32] Lucchini, A. Generators and minimal normal subgroups. *Arch. Math* **64** (1995) 273–276.

[33] Lucchini, A. Enumerating transitive finite permutation groups. *Bull. London Math. Soc.* **30** (1998) 569–577.

[34] Lucchini, A. Generating minimally transitive groups. *Proceedings of the Conference on Groups and Geometries, Siena, September 1996* (ed. A. Pasini, Birkhauser, Basel) (1998) 149–153.

[35] Lucchini, A.; Menegazzo, F.; Morigi, M. On the number of generators and composition length of finite linear groups. *J. Algebra* **243** (2001) 227–247.

[36] Lucchini, A.; Menegazzo, F. Generators for finite groups with a unique minimal normal subgroup *Rend. Sem. Math. Univ. Padova* **98** (1997) 173–191.

[37] Lucchini, A.; Menegazzo, F.; Morigi, M. Asymptotic results for transitive permutation groups. *Bull. London. Math. Soc.* **32** (2000) 191–195.

[38] Lucchini, A.; Morigi, M. Recognizing the prime divisors of the index of a proper subgroup. *J. Algebra* **337** (2011) 335–344.

[39] Maróti, A. On the orders of primitive groups. *J. Algebra* **258 (2)** (2002) 631–640.

[40] McIver, A.; Neumann, P.M. Enumerating finite groups. *Quart. J. Math. Oxford Ser.* (2) **38** (1987), 473–488.

[41] Menegazzo, F. The number of generators of a finite group. *Bull. Irish Math. Soc.* **50** (2003) 117–128.

[42] Neumann, P.M.; Vaughan-Lee, M.R. An essay on BFC-groups. *Proc. London. Math. Soc.* **35** (1977), 213–237.

[43] Praeger, C.; Saxl, J. On the order of primitive permutation groups. *Bull. London Math. Soc.* **12** (1980) 303–308.

[44] Pyber, L. Enumerating finite groups of given order. *Ann. Math.*, **(2) 137** (1993), 203–220.

[45] Pyber, L. Asymptotic results for permutation groups. *Groups and Computation* DIMACS Ser. Discrete Math. Theoret. Computer Sci. **11** (ed. Finkelstein, L. and Kantor, W.M., Amer. Math. Soc., Providence, 1993) 197–219.

[46] Rosser, J.B.; Schoenfeld, L. Approximate formulas for some functions of prime numbers. *Illinois J. Math.* **6** (1962) 64–97.

[47] Shepperd, J.A.M.; Wiegold, J. Transitive groups and groups with finite derived groups. *Math. Z.* **81** (1963) 279–285.

[48] Suprunenko, D.A. *Matrix Groups*. Translations of Mathematical Monographs, 45. Amer. Math. Soc., Providence, 1976.

[49] Tracey, G.M. Generating minimally transitive permutation groups. *J. Algebra* **460** (2016) 380–386.